Análisis de Malware

Comprensión y Análisis de Código Malicioso

Uso de herramientas, búsqueda en logs, funcionalidad y propósito del malware.

SECCION 3
Laboratorio de Análisis.

Clase 2
Sandbox y Análisis Dinámico.

.

Un sandbox es un **mecanismo de seguridad para disponer de un entorno aislado del resto del sistema operativo**.
Todos los programas que se ejecutan dentro de un sandbox lo hacen de forma controlada mediante los siguientes aspectos:

1.Se les asigna un espacio en disco. Podemos hacer que nuestros programas se ejecuten en un sistema de archivos temporal (tmpfs) para aislarlos del resto del sistema operativo.
2.También se les asigna un espacio en memoria. Los programas no podrán acceder a otras partes de la memoria que no les hayan sido asignadas.
3.Les podemos dar o restringir la capacidad para acceder y consultar dispositivos de almacenamiento externos.
4.Les restringimos la capacidad para que puedan inspeccionar la máquina anfitrión.
5.Podemos restringir el acceso de los programas a la red, al servidor de las X, al servidor de sonido, etc.
6.Podemos limitar el ancho de banda que usa un determinado programa.
7.Etc.

Consecuentemente podemos afirmar que los programas se ejecutan en un entorno controlado y separado del sistema operativo. Por lo tanto el hecho de ejecutar un programa en un sandbox es un ejemplo específico de VIRTUALIZACIÓN

VIRTUALIZADO EN…

LABORATORIO


CRACKS
DATA VIRUS
MALICIOUS SOFTWARE
THEFT
SOCIAL MEDIA ATTACKS
CYBERWARFARE
VIRUS
SOFTWARE FAILURE
NETWORK SNIFFING
YOUR DATA SAFETY
SPYWARE
HUMAN ERROR
SOFTWARE ERROR
STOLEN INFORMATION
TROJAN
CYBER ATTACKS
PASSWORD CRACKING
HACKING
FRAUD
CYBERCRIMINALS
TROJAN
ADWARE
SYSTEM PENETRATION
CYBERSTALKING

¡Nos vemos en la siguiente Clase!