Análisis de Malware

Comprensión y Análisis de Código Malicioso

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

SECCION
Laboratorio de Análisis.

Clase 1

Software de Virtualización.

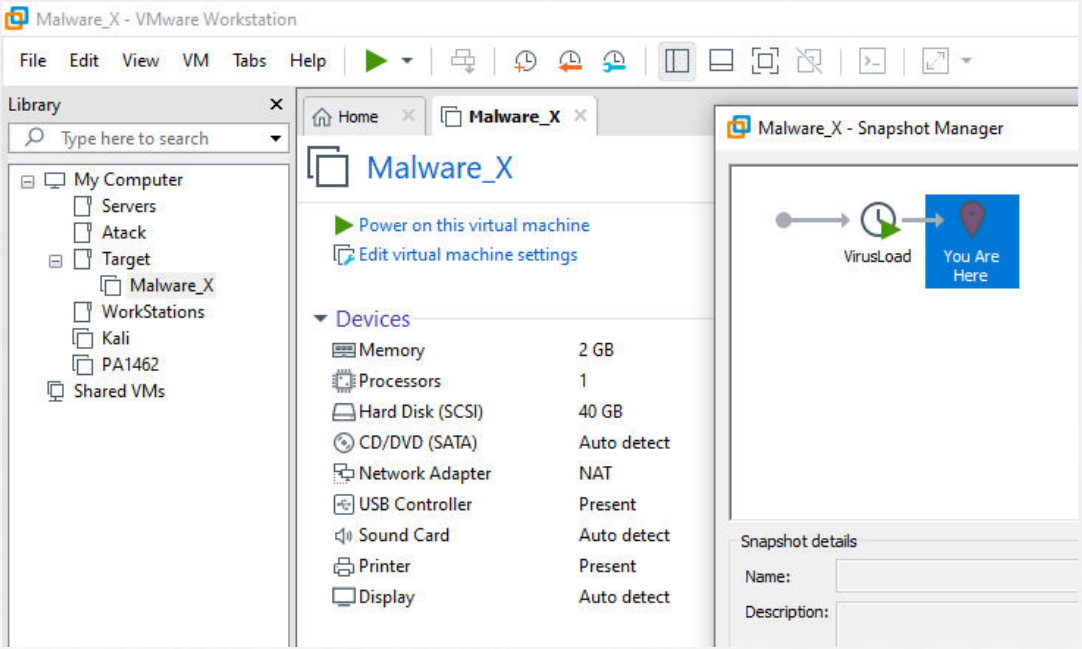
.

Para poder analizar necesitamos un entorno de trabajo, este entorno puede ser configurado por el propio analista, lo primero que puedes hacer es instalar y ejecutar algún software de virtualización como VMware o VirtualBox e instalar algún OS para dejarlo de laboratorio, por lo general utilizar un entorno de Windows puede ser útil debido a que hay muchas amenazas para estos sistemas.

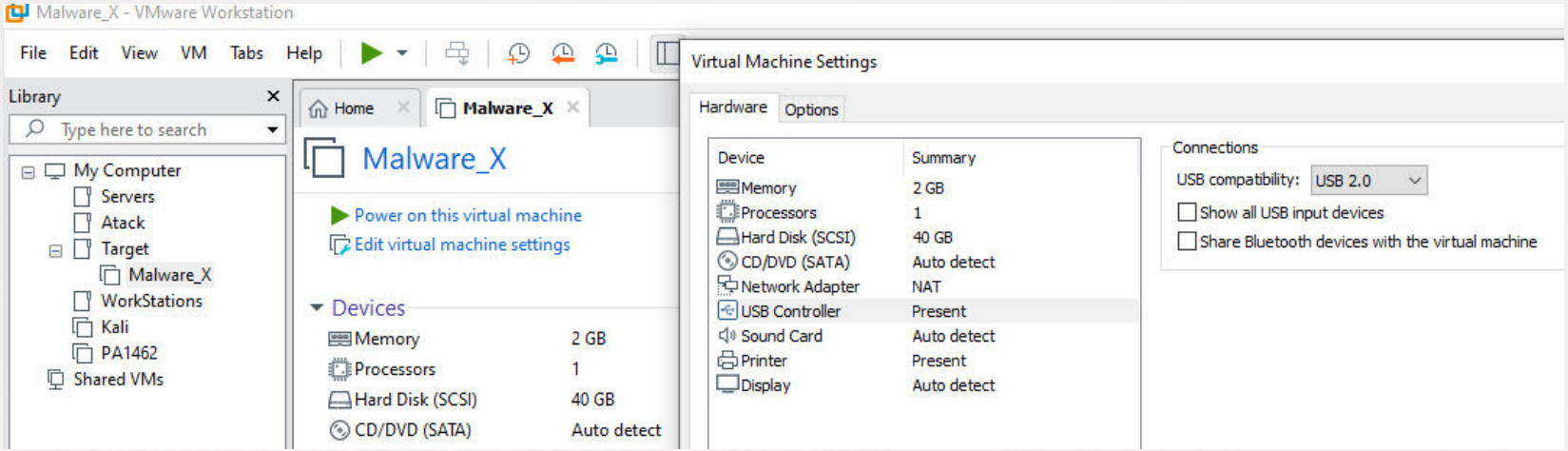
Una vez montada alguna imagen ISO (Windows en este caso), debemos tener en consideración lo siguiente:

Snapshot o clone:

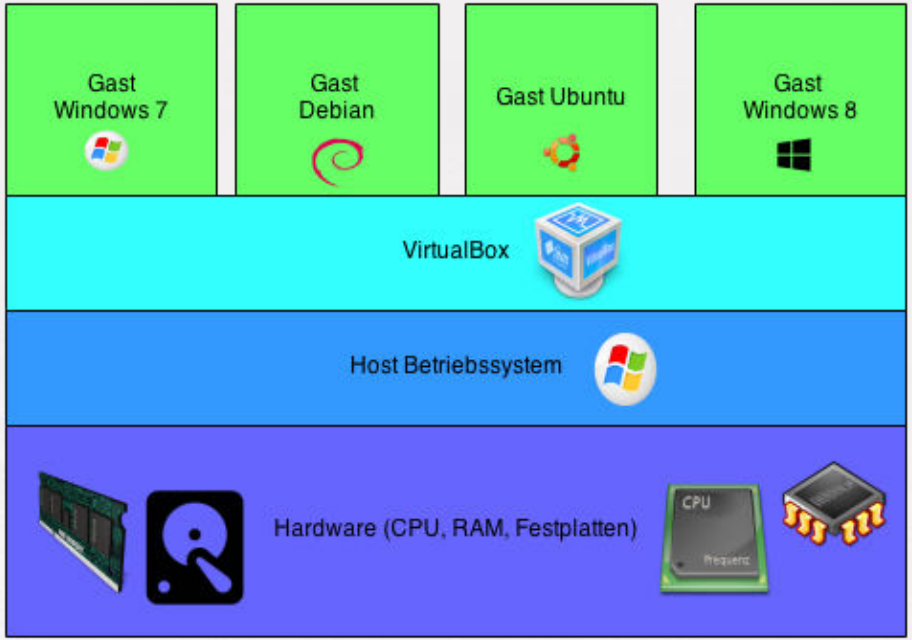
Toma un snapshot o clona tu máquina virtual, esta no debe ser única por ende siempre ten un respaldo para poder ir comparando comportamientos o simplemente volver a cero luego del análisis.



- Deshabilitar USB
  Hay malware que se propaga por medios de extracción USB si no eres cuidadoso quizás puedas infectar este tipo de dispositivos de estar conectado al momento del análisis. (También puedes ocupar un USB para descargar el Malware que quieres analizar, luego de eso deshabilitar)



- Ningún tipo de conexión con el anfitrión
  El anfitrión es el computador base, desde donde virtualizas, trata de que al momento del análisis no existan carpetas compartidas donde un malware podría pivotear entre equipos.




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!