Práctica 3: Antivirus LIVE

Este tipo de herramientas pueden ser muy útiles para tratar de desinfectar una máquina o como “segunda opinión” para contrastar la fiabilidad de otro antivirus. Hay que tener en cuenta que al tratarse de una distribución que se crea de forma periódica, la base de datos de los virus suele estar obsoleta y hay que actualizarla.

Podéis encontrar referencias a los más populares antivirus live por ejemplo en este artículo. Podéis usar cualquiera de ellos. En realidad todas las casas de antivirus disponen de este tipo de herramientas.

Esta es la forma correcta de verificar un sistema que pueda haberse infectado de un virus bien por no tener antivirus o por no tenerlo en condiciones. **Es muy poco probable que un antivirus ejecutado dentro de un sistema comprometido detecte una infección. Si el malware está activo antes de que el antivirus se inicie, probablemente se defenderá de éste y evitará ser detectado o eliminado.** La forma correcta es escanear la unidad comprometida desde otro Sistema Operativo. Esto se puede hacer con un antivirus live (ya que al arrancar desde la unidad externa, el virus no estará activo; además son sistemas Linux) o sacando el disco duro y conectándolo a otro sistema que tenga un antivirus de confianza como unidad externa.

Prueba al menos con la versión iso de uno de ellos en una máquina virtual con Windows. La máquina Windows debe tener instalado alguno de los malwares de ejemplo vistos en las prácticas anteriores. Si tienes un Windows que pueda estar contaminado puedes intentar diagnosticarlo, por supuesto.

Entrega una breve memoria que muestre las pruebas efectuadas. En particular deberíais de capturar la detección del keylogger, el eicar...