Computação Forense – Exercícios – Lista 06

Questões

1. O que é um Malware?
2. Quais as formas de obter um Malware e quais os danos que ele pode causar ao computador ou ao dono do computador?
3. Quais são as formas de estudar um Malware? Dê um exemplo de cada.
4. Procure na Internet e cite três exemplos de programas para (acrescente suas licenças):
   a) *Disassembler*;
   b) *Decompiler*;
   c) Editores de binário em hexadecimal;
   d) Analisadores de programas PE;
   e) *Debugger*;
   f) Emuladores;
   g) *Sniffers*;
   h) *Dumps* de memória;
   i) Backup e comparação do registro do Windows;
   j) Verificação de modificação de arquivos.
5. Baixe os seguintes programas de análise de Malware, instale-os no seu computador ou em uma máquina virtual, descreva suas funcionalidades e cite qual análise que ele pode ser utilizado para analisar (estática, dinâmica, post-mortem) um programa:
   a) https://hshrzd.wordpress.com/pe-bear/
   b) https://www.immunityinc.com/products/debugger/
   c) https://www.hex-rays.com/products/ida/support/download.shtml (baixe o freeware)
   d) http://www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm#download
   e) http://www.ollydbg.de/download.htm
6. Explique com exemplos quais são os perigos da análise dinâmica.
7. Explique o conceito de análise em *sandbox* e dê um exemplo de como fazê-la. Explique os perigos de fazê-la.
8. Explique, com um exemplo, o funcionamento de um monitor de chamadas de sistema.
9. Como fazer o confinamento somente de chamadas de sistema contidas em bibliotecas externas ao programa alvo?
10. O que é um ataque de *buffer overflow* (https://goo.gl/EZdeZo).

Para conhecimento:

Encontrei essa distribuição GNU/Linux e parece ser interessante: https://remnux.org/