Computação Forense – Exercícios

CCA UFES – Departamento de Computação
Prof. Msc. Jacson Rodrigues

Questões

Malwares (slides 06)

1. Sobre a análise de *malwares*: o que é e quando deve ser utiliza a análise estática, a análise dinâmica e a análise *post-mortem*?
2. O que é uma caixa de areia? Como criá-la? Como utilizá-la? Quais são seus perigos?
3. O que são monitores de chamada de sistema? Dê um exemplo de sua utilização/funcionamento.
4. O que é um *spoofing* de chamada de sistema? Dê um exemplo de sua utilização/funcionamento.
5. Como efetuar análise dinâmica de bibliotecas?
6. Quais são as características que complicam a análise de um software?

Ataques em Redes de Computadores (slides 08)

1. Quais são os tipos de invasores existentes e quais são os fatores que levam a uma invasão?
2. Quais são os passos que envolvem um ataque?
   a) Em quais passos o atacante pode ser identificado de forma mais fácil? Por quê?
   b) Em quais passos o atacante pode ser identificado de forma mais difícil? Por quê?
3. Quais são as atividades do processo de reconhecimento?
4. Quais são as atividades do processo de exploração?
5. Quais são as atividades do processo de reforço?
6. O que é *backdoor* e para que é utilizado?
7. Quais tipos de programas que podem detectar os *backdoors*? Esses programas sempre podem detectar os *backdoors*? Por quê?
8. "Um *backdoor* é normalmente instalado através da adição de um novo serviço ao sistema". Explique o que é um serviço e como o *backdoor* poderia ser fornecido.
9. Dê um exemplo de *backdoor*.
10. Quais são as atividades do processo de consolidação?
11. Quais são as atividades do processo de saque?
12. Quais os passos de um processo de segurança? Descreva cada um deles.
13. Descreva os principais tipos de ataques (utilize os slides como indicação).