Simulado de Prova II de Segurança da Informação, 26-jun-2019
Turma 2019/1, IC/UFF, Prof. Raphael Machado

1. Explique resumidamente cada um dos ataques abaixo:
   - Injeção de SQL
   - Buffer Overflow
   - Format String

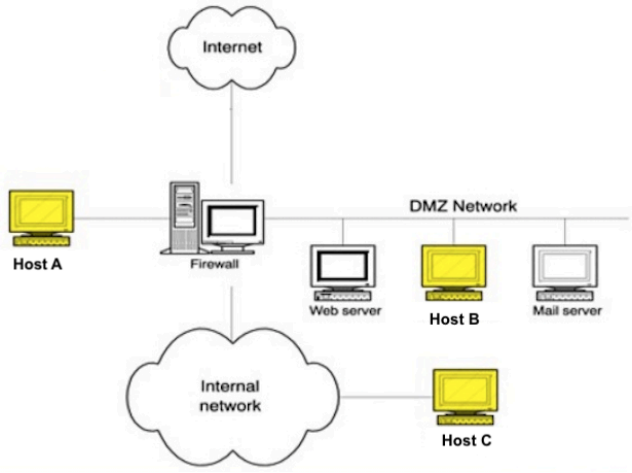
2. Explique o que são “bases de vulnerabilidades” e dê dois exemplos de tais bases.

3. Descreva brevemente o que é um SIEM.

4. Descreva as diferenças entre um IDS baseado em estação e um IDS baseado em rede. Que tipos de dados são usados em cada tipo de IDS para realizar detecções.

5. Um pesquisador desenvolveu um sistema de detecção de intrusão para uma rede sem fio. O pesquisador observou que o sistema desenvolvido apresentava um alto número de alertas indevidos (falsos-positivos) e mudou um parâmetro de threshold até um valor que levasse a um número de falsos-positivos aceitável. Você acredita que essa modificação pode levar o sistema a ser mais facilmente atacado? Justifique sua resposta.

6. Um administrador de redes de uma organização posicionou em sua rede alguns computadores propositalmente vulneráveis (hosts A, B e C). Esses computadores não eram responsáveis pode nenhuma atividade produtiva da organização.



Após um mês de operação nessa configuração, o administrador observou uma série de acessos aos hosts A, B e C e passou a investigar tais acessos. Responda às seguintes perguntas.

a) Que tipo de acessos espera-se que o administrador de redes observe nos hosts A, B e C?
b) Esperam-se diferenças entre os acessos observados nos hosts A, B e C? Explique
c) Qual o nome do “conceito” que o administrador de redes está usando para estudar a segurança da rede – ou seja, através da inclusão, na rede, de hosts vulneráveis, com o objetivo de estudar as tentativas de acesso a tais hosts?

7. Cite quatro tipos diferentes de firewall e descreva brevemente as características de cada um.

8. Discuta brevemente a diferença entre os padrões ISO/IEC 27001 e ISO/IEC 27002.

9. Cite dois padrões de segurança da informação aplicáveis a “produtos de software” com alcance internacional. Descreva brevemente o escopo de cada um deles.

10. Explique por que laboratórios que realizam ensaios de software no escopo do Common Criteria precisam ser acreditados no âmbito da ISO/IEC 17025.