Avaliação Parcial I

Auditoria e Segurança de Sistemas de Informação 8,0

Prof. Roberto Cabral

26 de maio de 2023

Aluno: [ ] Matrícula: [-]

1,5

1. (1,5 ponto) Descreva e defina as propriedades básicas da segurança da informação. Explique cada propriedade em detalhes e forneça exemplos relevantes.

1,5

2. (1,5 ponto) Defina o que é um *ransomware*. Quais as formas mais comuns de propagação? Caso seu equipamento seja infectado, o que pode ser feito para acessar novamente os arquivos?

1,0

3. (2 pontos) Uma cifra de substituição monoalfabética é um método de criptografia que opera de acordo com um sistema pré-definido de substituição. A cifra de substituição simples pode ser expressada pelo embaralhamento do alfabeto.

   (a) Essa cifra pode ser considerada segura?

   (b) Qual a dificuldade do ataque de força bruta à esse criptosistema?

   (c) Existe algum ataque mais prático? Se sim, qual?

   (d) Qual as duas propriedades principais que uma boa cifra deve ter? Por quê?

4. (6 pontos) Marque V nas alternativas corretas e F nas alternativas falsas.

Observações:

- Cada item correto vale 0,5.
- Um item errado vale -0,5.
- Um item não respondido não afeta a nota.
- **CUIDADO!** Sua nota na questão pode ser negativa.

4,0

(a) (F) Um ataque a um Sistema de Informação é um ato intencional que pode causar danos ou comprometer informações e/ou os sistemas que as suportam.

(b) (F) Um equipamento pode ser infectado ou comprometido pela execução de arquivos legítimos.

(c) (F) Cavalo de Troia é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e com o conhecimento do usuário.

(d) (V) Um *Backdoor* é um programa que permite o retorno de um invasor a um equipamento comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

(e) (F) *Boatos sempre contêm informações falsas.*

(f) (V) Boatos são disseminados por pessoas mal-intencionadas com o objetivo de prejudicar outros indivíduos ou grupos.

(g) (F) Em um cripto-sistema simétrico, sempre é possível construir um ataque prático usando força bruta.

(h) (V) A construção esponja é dividida nas fases de inicialização, absorção e extração.

(i) (V) O tamanho da saída de uma função de resumo criptográfico afeta sua segurança.

(j) (V) É impossível, no cenário atual, quebrar a criptografia assimétrica através de um ataque de força bruta.

(k) (V) Se um algoritmo criptográfico é computacionalmente seguro em relação a força bruta, podemos afirmar que ele é computacionalmente seguro.

(l) (F) Um cripto-sistema é incondicionalmente seguro se apenas for possível quebrá-lo com recursos computacionais infinitos.

4,0

Boa Sorte!