

Aluno: Roberto Abreu Bento

**Instruções e Observações:**

- 1 - A interpretação da prova faz parte da avaliação.
- 2 - Não é permitido ausentar-se da sala durante a realização da avaliação.
- 3 - Não é permitido o uso de celulares, microcomputadores e calculadoras programáveis durante a prova.
- 4 - Não é permitido consultar qualquer tipo de material durante a prova.
- 5 - Somente será permitido consulta a ... (materiais definidos pelo professor).
- 6 - Respostas sem apresentação do desenvolvimento ou com desenvolvimento incompatível serão consideradas incorretas.
- 7 - Perguntas sobre o conteúdo e correção das questões não serão respondidas no decorrer da prova. Caso tenha alguma dúvida quanto ao enunciado da questão, levante sua mão e aguarde em silêncio pelo professor.
- 8 - A cola será penalizada com nota zero.

1) Com relação à segurança da informação, assinale a opção correta.

☒ a) *Backdoor* Permite o acesso em uma máquina a um invasor de computador, pois assegura a acessibilidade a essa máquina em modo remoto.

b) *Worm* é um programa ou parte de um programa de computador, usualmente malicioso, que se propaga ao criar cópias de si mesmo e, assim, se torna parte de outros programas e arquivos.

c) *Cookie* é um programa capaz de se propagar, automaticamente, por rede, pois envia cópias de si mesmo de computador para computador, por meio de execução direta ou por exploração automática das vulnerabilidades existentes em programas instalados em computadores.

d) *Spyware* é um programa que permite o controle remoto do agente invasor e é capaz de se propagar automaticamente, pois explora vulnerabilidades existentes em programas instalados em computadores.

e) *Vírus* é um programa que monitora as atividades de um sistema e envia informações relativas a essas atividades para terceiros. Um exemplo é o vírus *keylogger* que é capaz de armazenar os caracteres digitados pelo usuário de um computador.

2) Na virada do mês de janeiro para fevereiro de 2012, os sites de diversos bancos comerciais brasileiros foram alvos de ataques através da Internet com o objetivo de deixá-los inacessíveis. O tipo de ataque de que foram vítimas estes bancos é conhecido genericamente pelo nome de:

a) *Spoofing*.

b) *backdoor*.

c) *cookie*.

☒ d) *denial of service (Dos)*.

e) *phishing*.

3) *IPspoofing* é uma técnica utilizada para mascarar pacotes IP por meio de endereços errados, a fim de que não seja possível identificar o endereço IP e para que não se permita a identificação do invasor.

☒ a) Certo      b) Errado

4) Com relação aos princípios de criptografia, analise as afirmativas a seguir.



I. Na criptografia simétrica, a mesma chave é utilizada para encriptar e decriptar a mensagem, devendo a mesma ser acordada entre o transmissor e o receptor.

II. A criptografia assimétrica dá origem à figura das chaves pública e privada

III. Da mesma forma que na criptografia simétrica, na assimétrica é necessário um acordo prévio de chaves entre o transmissor e o receptor.

Assinale:

- 1.25
- c
- a) se somente a afirmativa I estiver correta.
  - b) se somente a afirmativa II estiver correta.
  - c) se somente a afirmativa III estiver correta.
  - ☒ d) se somente as afirmativas I e II estiverem corretas.
  - e) se todas as afirmativas estiverem corretas.

1.25

5) O uso de assinatura digital, além de prover autenticidade e integridade, também permite o repúdio da informação, tendo em vista que o emissor pode negar a emissão da mensagem.

- c
- a) Certo      ☒ b) Errado

6) Em assinatura digital, a função hashing:

- 9.0
- X
- ☒ a) utiliza um algoritmo cuja função é produzir um valor hash de 64 bits para uma mensagem de tamanho arbitrário.
  - b) é utilizada para gerar um valor de chave privada, a partir da criptografia simétrica.
  - c) funciona como uma impressão digital de uma mensagem, gerando, a partir de um valor de tamanho fixo, uma chave de tamanho variável.
  - d) é utilizada para gerar um valor pequeno, de tamanho fixo, derivado da mensagem que se pretende assinar.
  - e) utiliza o algoritmo DES de chave pública e privada

9.0

7) Com relação aos requisitos de segurança da informação, assinale a opção correta.

- X
- 1.25
- a) A integridade é diretamente obtida quando se tem a confidencialidade.
  - b) A disponibilidade não é afetada pela obtenção da integridade e da confidencialidade.
  - c) A integridade requer que a informação só seja acessada por quem estiver autorizado.
  - ☒ d) A confidencialidade garante que a informação não será alterada por quem não estiver autorizado.
  - e) A adição da integridade a um sistema com confidencialidade eleva o seu nível de segurança.

c

8) A segurança da informação pode ser entendida como uma atividade voltada à preservação de princípios básicos, como confidencialidade, integridade e disponibilidade da informação

- ☒ a) Certo      b) Errado