1)

Os sistemas distribuídos tem como objetivo a segurança, nele temos uma seria de componentes, hardwares e softwares, que se comunicam para a execução de aplicações.

Com relação aos sistemas distribuídos, analise o excerto a seguir, completando suas lacunas.

Uma das formas mais funcionais de se prevenir nossos sistemas atualmente é utilizando uma estratégia de segurança \_\_\_\_\_\_\_\_\_\_. Este tipo de estratégia \_\_\_\_\_\_\_\_\_\_ com diferentes tecnologias de segurança os principais pontos de entrada de ameaças. A segurança multicamada \_\_\_\_\_\_\_\_\_\_ consideravelmente o grau de dificuldade para uma invasão de um intruso, \_\_\_\_\_\_\_\_\_\_ drasticamente o risco de um \_\_\_\_\_\_\_\_\_\_ ter acesso indevido à rede e dados de empresas.

Assinale a alternativa que preenche corretamente as lacunas.

**Alternativas:**

* a)

multicamadas / protege / diminui / aumentando / hacker.

* b)

monocamadas / lida / aumenta / reduzindo / analista.

* c)

multicamadas / alterna / aumenta / aumentando / analista.

* d)

monocamadas / protege / diminui / reduzindo / hacker.

* e)

multicamadas / protege / aumenta / reduzindo / hacker.

Alternativa assinalada

2)

Ameaças são ações praticadas por softwares projetados com intenções danosas, e para produzir um sistema que seja seguro contra diversas ameaças, é necessário classifica-las e entender seus  métodos de ataque. As ameaças aos sistemas distribuídos podem ser divididas em algumas classes.

COULOURIS, G. et al. Sistemas Distribuídos. Porto Alegre: Bookman, 2013.

Considerando o contexto, avalie as afirmativas a seguir:  
I. Leakage (vazamento) é o acesso a informação por agentes não autorizados.  
II. Tampering (falsificação) é a modificação não autorizada de uma informação.  
III. Vandalism  (vandalismo) é a interferência no  funcionamento de  um  sistema  sem  ganhos  para  o criminoso.

Considerando o contexto apresentado, é correto o que se afirma em:

**Alternativas:**

* a)

I e II, apenas.

* b)

I e III, apenas.

* c)

II e III, apenas.

* d)

I, apenas.

* e)

I, II e III.

Alternativa assinalada

3)

Ameaças são ações praticadas por softwares projetados com intenções danosas, e para produzir um sistema que seja seguro contra diversas ameaças, é necessário classifica-las e entender seus  métodos de ataque, porem existem estratégias de violações de segurança em sistemas distribuídos, que dependem da obtenção de acesso aos canais de comunicação do sistema com a autoridade desejada.

Assinale a alternativa que apresenta corretamente a estratégia.

**Alternativas:**

* a)

Message tampering (falsificação de mensagem) é o acesso a cópias de mensagem sem autorização. Geralmente essa estratégia funciona através da captura de mensagens da rede.

* b)

Eavesdropping ocorre quando a máquina do invasor faz envio ou recebimento de mensagens utilizando a identidade de outra máquina autorizada pela aplicação.

* c)

Masquerading (disfarce) ocorre quando a máquina do invasor faz a captura e alteração do conteúdo das mensagens e após isso faz a transferência ao destinatário.

* d)

Replaying é quando o invasor consegue fazer a captura e armazenamento das mensagens por um período de tempo, utilizando para isso o envio atrasado das mensagens aos seus destinatários.

Alternativa assinalada

* e)

Worm é um programa oferecido aos usuários através de um sistema que mostra ser capaz de utilizar uma função útil, mas que tem uma segunda intenção que vem oculta através de uma função