7ª. Lista de Exercícios de Segurança de Sistemas
Prof. Manoel Ribeiro

1)Em relação à vulnerabilidades e ataques a sistemas computacionais, é correto afirmar:

a) Medidas de segurança podem ser definidas como ações que visam eliminar riscos para evitar a concretização de uma vulnerabilidade.
b) O vazamento de informação e falha de segurança em um software constituem vulnerabilidades.
c) Roubo de informações e perda de negócios constitui ameaças.
d) Medidas de segurança podem ser definidas como ações que visam eliminar vulnerabilidades para evitar a concretização de uma ameaça.
e) Área de armazenamento sem proteção e travamento automático da estação após período de tempo sem uso constituem ameaça.

2) Qual das seguintes opções refere-se, exclusivamente, a classes de ataques ativos à Segurança de Informações?
A Liberação de conteúdo da mensagem; Análise de Tráfego; Negação de Serviço.
B Disfarce; Análise de Tráfego; Negação de Serviço.
C Análise de Tráfego; Liberação de Conteúdo da mensagem; Negação de Serviço.
D Disfarce; Modificação de conteúdo das Mensagens; Negação de Serviço.
E Liberação de conteúdo da mensagem; Modificação de conteúdo da mensagem; Mudança de autenticidade de remetente.

3)Um ambiente com alto nível de informatização e alta concentração de informações acessíveis por sistemas automatizados apresenta baixa vulnerabilidade técnica e baixa dependência de uma política de classificação de informações, que tem por objetivo identificar informações valiosas e assegurar um grau mínimo de proteção para essas informações.

C Certo
E Errado

4) Sobre os conceitos de segurança da informação, analise as afirmativas a seguir:
I. Uma ameaça tem o poder de comprometer ativos vulneráveis.
II. Risco é a combinação das consequências de um incidente de segurança com a sua probabilidade de ocorrência.
III. Vulnerabilidades técnicas são mais críticas do que vulnerabilidades criadas por comportamento humano.
Está correto somente o que se afirma em:
A I;
B II;
C III;
D I e II;
E I e III.

5) Uma boa política de segurança da informação envolve diversas ações preventivas. Vulnerabilidade e ameaças sempre estarão lado a lado, pois caso haja uma vulnerabilidade em um sistema, certamente existirá a possibilidade de uma ameaça. Uma infraestrutura de TI pode ser subdivida em sete domínios, que estará sujeita a alguma vulnerabilidade. Duas vulnerabilidades muito comuns e usadas para atividade criminosa são: acesso de usuário não autorizado e falhas em software instalado. O domínio de infraestrutura de TI que essas vulnerabilidades estão relacionadas é:
A Domínio de usuário.
B Domínio de acesso remoto.
C Domínio de sistema/aplicativo.
D Domínio de estações de trabalho.

6) Em segurança da informação, NÃO é considerada uma causa de vulnerabilidade:
A imaturidade em segurança.
B percepção de simplicidade.
C restrições de recursos.
D desenvolvimento in-house.

E controle de tempo.

7) Com relação à segurança da informação, assinale a opção correta.
A A política de segurança da informação define o que deve ser protegido, por quê, e também quem será o responsável pela proteção, provendo uma base para decisões futuras.
B A avaliação de riscos deve abranger o que deve ser protegido e contra o quê. Porém, não deve levar em consideração o esforço, o tempo e os recursos necessários.
C Vulnerabilidade é uma feature de um software que, quando explorada, pode levar a comportamento não desejado.
D O risco de um ataque é proporcional à sua facilidade de execução.
E A ameaça é o produto do risco pelo custo da proteção.

8) Indique a alternativa que pode conter um relacionamento mais apropriado entre os conceitos de AMEAÇA, IMPACTO, INCIDENTE e VULNERABILIDADE tratados pela Gestão de Riscos na Tecnologia da Informação.
A

ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Servidor de aplicação	Falta de atualizações do sistema operacional	Exploração de vulnerabilidades conhecidas	Perda de Confidencialidade, Integridade e Disponibilidade

B

ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Servidor *Web*	Servidor de aplicação acessível pela internet	Ataque *Hacker* DDoS	Integridade

C

ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Firewall da rede	Sem contrato de manutenção periódica	Defeito no *firmware*	Perda da confidencialidade nos acessos a internet

D

ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Servidor *Web*	Ataque *Hacker* DDoS	Falta de atualizações do sistema operacional	Indisponibilidade

E

ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Firewall da rede	Falta de atualizações do IOS	Perda de desempenho	Não suporta atualizações de *hardware*

9) Considere o texto abaixo.

Treze dos mais populares roteadores usados em casa e em pequenos escritórios contêm problemas de segurança que poderiam permitir que um cracker "bisbilhotasse" ou modificasse o tráfego da rede. A empresa de consultoria de segurança Independent Security Evaluators (ISE) descobriu que todos os roteadores que testaram poderiam ser controlados caso o cibercriminoso tivesse as credenciais de acesso. Os consumidores têm poucas opções para mitigar os ataques, disse a ISE em seu relatório. "Uma mitigação bem sucedida requer, muitas vezes, um nível de sofisticação e habilidade além do que tem o usuário médio", disse a ISE.

10) O termo utilizado no texto, com vistas ao tratamento do risco significa
A não adotar nenhum procedimento para evitar a possibilidade de serem bisbilhotados.
B adotar procedimentos para eliminar a possibilidade do tráfego da rede ser modificado.
C adotar procedimentos para minimizar a possibilidade de serem bisbilhotados.
D contratar um consultor especializado em Segurança de Tecnologia da Informação.
E delegar a solução do problema para uma empresa parceira.