O termo “Engenharia Social” é comumente utilizado para se referir a técnicas utilizadas por pessoas mal-intencionadas que abusam de relações sociais para conseguir informações sigilosas ou acesso a sistemas. Dos cenários abaixo, NÃO caracteriza um caso de Engenharia Social o que está descrito em

a) Em um ambiente de trabalho, uma pessoa liga, identifica-se como administrador dos sistemas da empresa e solicita que você siga uma série de passos, incluindo acesso a sites na internet e instalação de softwares, para melhorar o desempenho da sua máquina.

b) Você recebe um e-mail indicando que acaba de ser sorteado com um prêmio e instruindo-o a acessar um determinado site e preencher o cadastro para coletar o seu prêmio.

c) Você recebe um e-mail alertando sobre um novo vírus muito perigoso e orientando-o a procurar por determinado arquivo em seu sistema e, caso ele exista, excluí-lo imediatamente e repassar a mensagem a todos os seus conhecidos.

d) Uma pessoa liga para você, identifica-se como sendo de uma empresa prestadora de serviços (ex.: de telefonia), explica que há um problema no seu cadastro e pede que você informe vários dados pessoais, como nome completo, endereço, etc.

e) Após fornecer seu endereço de e-mail em um site para se cadastrar, você recebe uma mensagem de e-mail desse site pedindo que você clique em um link para confirmar o seu cadastro.

Em relação a 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.

Analise as seguintes afirmações relacionadas a Segurança da Informação:

I. Uma Vulnerabilidade é um evento com consequências negativas resultante de um ataque bem-sucedido.

II. Uma Ameaça é uma expectativa de acontecimento acidental ou proposital, causada por um agente, que pode afetar um ambiente, sistema ou ativo de informação.

III. A Vulnerabilidade é uma fonte produtora de um evento que pode ter efeitos adversos sobre um ativo de informação.

IV. O Ataque é um evento decorrente da exploração de uma vulnerabilidade por uma ameaça.

Indique a opção que contenha todas as afirmações verdadeiras.

a) I e II.
b) II e III.
c) III e IV.
d) I e III.
e) II e IV.

Com relação a ataques DoS (Denial of Service) e DDoS (Distributed Denial of Service), analise:

I. O ataque DoS (Denial of Service), é também denominado ataque de negação de serviço.

II. No ataque DoS o atacante tenta tornar os recursos de um sistema indisponíveis para seus usuários.

III. DDoS, constitui um ataque de negação de serviço distribuído, ou seja, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet.

Marque a opção que apresenta apenas as afirmativas corretas:

a) Somente a I.
b) Somente II e III
c) Somente a III.
d) Somente I e II
e) I, II e III.

Acerca das tecnologias de segurança e dos ataques eletrônicos, julgue os itens a seguir.

Uma das propriedades de uma função de hash, conhecida como resistência à primeira inversão ou propriedade unidirecional, garante que, dada uma mensagem, não é possível encontrar uma mensagem alternativa que gere o mesmo valor de hash da mensagem original.

( ) Certo

( ) Errado

Vários problemas de segurança surgiram a partir do crescimento das redes. Como exemplo destes problemas temos roubo de senhas e interrupção de serviços até problemas de personificação, onde uma pessoa faz-se passar por outra para obter acesso privilegiado. Surgiu então a necessidade do aprimoramento do processo de autenticação, que consiste na verificação da identidade dos usuários.

Com relação a este assunto são realizadas as seguintes afirmativas:

1. A verificação ou autenticação em duas etapas (two-factor authentication, também chamada de aprovação de login, verificação ou autenticação em dois fatores ou, ainda, verificação ou autenticação em dois passos) adiciona uma segunda camada de proteção no acesso a uma conta, dificultando que ela seja indevidamente acessada, mesmo com o conhecimento da senha. É um recurso opcional oferecido por diversos serviços de Internet, como Webmail, redes sociais, Internet Banking e de armazenamento em nuvem.

2. Na verificação em duas etapas são utilizados dois passos de checagem, ou seja, é feita uma dupla verificação. Adicionando uma segunda etapa de verificação fica mais difícil a invasão de uma conta de usuário. Mesmo que um atacante venha a descobrir uma senha ela, isoladamente, não será suficiente para que ele consiga acessar a conta. O atacante necessitará executar a segunda etapa, o que tornará a invasão mais difícil de ser realizada.

3. Existem três grupos básicos de mecanismos de autenticação, que se utilizam de: aquilo que você é (informações biométricas, como a sua impressão digital, a palma da sua mão, a sua voz e o seu olho), aquilo que apenas você possui (como seu cartão de senhas bancárias e um token gerador de senhas) e, finalmente, aquilo que apenas você sabe (como perguntas de segurança e suas senhas).

Assinale a alternativa que indica todas as afirmativas corretas.

a) É correta apenas a afirmativa 1.
b) É correta apenas a afirmativa 2.
c) São corretas apenas as afirmativas 1 e 3.
d) São corretas apenas as afirmativas 2 e 3.
e) São corretas as afirmativas 1, 2 e 3.

Com relação a segurança da informação, um Firewall é:

a) um sistema que investiga a ocorrência de vírus em uma rede, ao varrer todos os computadores da rede procurando por arquivos infectados.

b) um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.

c) um conjunto de sistemas ‘nobreak’ que servem para garantir o funcionamento dos servidores quando falta energia.

d) um servidor que realiza a autenticação de todos os usuários da rede, requisitando contas e senhas, muitas vezes combinadas com autenticação biométrica.

e) um sistema baseado em protocolos sofisticados de criptografia que analisa todas as senhas utilizadas na rede local e garante que os usuários utilizem apenas senhas fortes.

Em segurança de redes de computadores, os firewalls atuam como filtros de pacotes. Eles inspecionam todo e qualquer pacote que entra e sai de uma rede. É INCORRETO afirmar que o firewall:

a) é uma configuração que isola algumas máquinas do resto da rede em que está ligado.

b) é uma descrição coletiva para vários métodos que restringem o acesso a uma rede.

c) previne contra ataques baseados em dados que envolvem alguma informação perigosa.

d) possui a definição de restrições na maneira como os pacotes da rede são roteados.