# AVALIAÇÃO - 02 - CARONTE

01 ) As tentativas de invasão às redes de computadores têm sido objeto de preocupação dos profissionais de segurança nas empresas. Uma técnica utilizada por fraudadores está caracterizada a seguir:

- Mensagens são enviadas por e-mail, que parecem ser originadas de instituições financeiras ou empresas idôneas, contêm um link falso que leva o cliente para um site também falso, mas muito parecido com o original da instituição financeira/empresa anunciada.
- O conteúdo do e-mail induz o cliente/usuário a fornecer dados pessoais e financeiros, por exemplo, por meio de falsa atualização de informações cadastrais. Nesse caso, os dados digitados pelo cliente, como, por exemplo, o número da sua agência, conta-corrente ou poupança, e senha, são capturados pelo cracker/hacker, e utilizado posteriormente.

Essa técnica é conhecida por
a) cookie.
b) phishing.
c) spoofing.
d) denial of service.
e) dumpster of service

02) FCC/2012 - Com relação ao tema criptografia, analise as asserções a seguir.

Maria criptografa a mensagem (texto claro) utilizando-se da chave privada de João. A mensagem cifrada é então enviada a João que a decriptografa utilizando sua chave pública. Como a criptografia assimétrica trabalha com funções matemáticas bidirecionais, João não conseguiria decriptografar a mensagem usando sua chave privada
**PORQUE**
Apenas a chave pública permite essa decriptografia, já que é gerada por algoritmos criptográficos assimétricos e é de conhecimento de ambos os envolvidos na troca de mensagens.

Acerca dessas asserções, é correto afirmar:
a) As duas asserções são proposições verdadeiras, e a segunda é a justificativa correta da primeira.
b) As duas asserções são proposições verdadeiras, mas a segunda não é a justificativa correta da primeira.
c) A primeira asserção é uma proposição falsa, e a segunda, uma proposição verdadeira.
d) A primeira asserção é uma proposição verdadeira, e a segunda, uma proposição falsa.
e) Tanto a primeira quanto a segunda asserções são proposições falsas.

03) A criptografia moderna tem três tipos de ferramentas básicas: algoritmos criptográficos simétricos e assimétricos e as funções de resumo de mensagem. Acerca dos principais algoritmos para esses tipos de ferramenta criptográfica, julgue o item subseqüente:

MD5 e SHA-1 são funções de resumo de mensagem (funções hash). Esses algoritmos têm a finalidade de garantir a integridade e a autenticidade para mensagens de tamanho arbitrário.

A) VERDADEIRO B) FALSO

04) FCC/2011 No contexto das ameaças e vulnerabilidades de rede, considere:

Cross-site Scripting (XSS) é uma vulnerabilidade em sites web que permite que um indivíduo malicioso execute código Javascript no site alvo no contexto do usuário e, dessa forma, poder roubar credenciais de acesso ou até executar comandos em nome do administrador.

A) CERTA B) ERRADA

05) Um dos esquemas criptográficos mais utilizados atualmente é o esquema conhecido como criptografia de chave pública. Neste esquema,

a) o emissor codifica a mensagem utilizando a chave privada e o receptor decodifica a mensagem utilizando a chave pública.
b) o emissor codifica a mensagem utilizando a chave pública e o receptor decodifica a mensagem utilizando a chave privada.
c) uma mesma chave pode fazer simultaneamente o papel de chave pública e de chave privada na comunicação, mediante prévio acordo entre emissor e receptor.
d) caso o sigilo da chave privada seja comprometido, é possível substituí-la, sem ser necessário substituir a chave pública.
e) não é possível implementar assinaturas ou certificados digitais.

06) Sobre criptografia é correto afirmar:
a) Na criptografia/descriptografia simétrica, a chave privada que é usada para criptografia é diferente da chave pública usada para decriptografia. A chave pública está disponível ao público geral; a chave privada fica disponível apenas para um indivíduo.
b) Na criptografia de chave assimétrica, a mesma chave é usada pelo emissor (para criptografia) e pelo receptor (para descriptografia). A chave é compartilhada.
c) A cifra de César é uma cifra de substituição que troca um símbolo por outro na mensagem, sem introduzir deslocamento.
d) Um hash também é conhecido como resumo de mensagem, serve, entre outros propósitos para garantir integridade.
e) Em uma cifra de substituição, há substituição de caracteres mas as posições não mudam.

07) Para se enviar uma mensagem criptografada do usuário A para o usuário B com a utilização de infraestrutura de chaves públicas, com o intuito de garantir a autenticidade da mensagem, é necessário que antes do envio o usuário A cifre a mensagem com
a) a chave privada de B.
b) sua chave pública.
c) a chave pública de B.
d) sua chave privada.
e) com a chave privada de B e com sua chave pública, respectivamente.

08) CESPE/2012 - Com respeito a vulnerabilidades e ataques a sistemas computacionais, julgue o item:
A técnica denominada SQL injection tem por objetivo o acesso a bancos de dados por meio de aplicações web. Ataques embasados nessa técnica podem ser evitados por checagem de dados de entrada no backend e frontend da aplicação.

A) VERDADEIRA B) FALSA

09) CESGRANGRIO/2010 - Uma aplicação WEB de uma empresa foi invadida e, após análise, descobriram que o ataque utilizou a técnica de SQL Injection. Sobre essa situação, afirma-se que:
a) filtros de pacote podem ser configurados como mecanismo de proteção eficiente.
b) a aplicação necessita de manutenção para correção desse tipo de falha.
c) o kernel do sistema operacional do servidor envolvido estava desatualizado.
d) o servidor envolvido precisará de mais placas de rede para evitar novos ataques.
e) o banco de dados envolvido sofreu, na ocasião, um DoS, tornando-se indisponível.

10) FCC/2009 - Considere o recebimento de um e-mail que informa o usuário a respeito de uma suposta contaminação do computador dele por um vírus, sugerindo a instalação de uma ferramenta disponível em um site da Internet para eliminar a infecção. Entretanto, a real função dessa ferramenta é permitir que alguém tenha acesso ao computador do usuário e a todos os dados lá armazenados. Este método de ataque trata-se de

a) Engenharia Social.
b) Sniffer.
c) Backdoor.
d) Exploit.
e) Denial of Service.

11) CESGRANRIO/2008 - Um administrador de rede percebeu que um dos componentes de software do kernel do seu servidor Web está apresentando um comportamento estranho. Após realizar um checksum no componente ele percebeu que o teste falhou e que a solução para o problema seria reinstalar todo o sistema operacional, pois, outros componentes do kernel também apresentaram o mesmo problema. Com base neste teste, conclui-se que o servidor sofreu um ataque do tipo:

a) spyware.
b) rootkit.
c) spoofing.
d) adware.
e) keylog.

12) FEPESPE/2010 - A segurança da informação protege as organizações contra uma ampla gama de ameaças, para assegurar a continuidade dos negócios, minimizar prejuízos e maximizar o retorno de investimentos e oportunidades comerciais. **(2PTS)**
A respeito dos conceitos de segurança da informação, assinale a alternativa correta.

a) Um sistema é dito seguro se garante as três propriedades básicas de segurança: confiabilidade, integridade e disponibilidade. A falha em um mecanismo de segurança é uma violação da confiabilidade; a modificação de uma informação em trânsito é uma violação da integridade; e a interrupção de um serviço oferecido pela rede é uma violação da disponibilidade.
b) Vulnerabilidades causadas por erro humano são as mais fáceis de explorar e as mais difíceis de prevenir e detectar. Ataques de engenharia social exploram esta vulnerabilidade e permitem que invasores obtenham informações sigilosas e privilegiadas. Treinamentos constantes sobre segurança são a contramedida mais eficiente para minimizar o sucesso destes ataques.
c) Para implantação de controles lógicos de acesso à rede, mecanismos de autenticação de equipamentos devem ser utilizados. Para este fim, podem-se empregar as técnicas baseadas em um segredo (senha), técnicas baseadas em perfis biométricos (impressão digital) e as técnicas que utilizam dispositivos especiais (smartcard).
d) Em uma organização que pretende implantar um sistema de gestão de segurança da informação, todos os ativos da informação devem ser classificados em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização. Esta classificação é suficiente para a correta seleção dos controles de segurança que os protegerão.
e) As áreas de segurança devem ser protegidas por controles físicos de entrada. Logo, deve-se implantar uma técnica de autenticação multifator que combine identificação e senha sempre que se deseja implantar autenticação forte dos usuários.

13) ESAF/2005 - Analise as seguintes afirmações relacionadas à segurança e uso da Internet:

I. Engenharia Social é um termo que designa a prática de obtenção de informações por intermédio da exploração de relações humanas de confiança, ou outros métodos que enganem usuários e administradores de rede.
II. Port Scan é a prática de varredura de um servidor ou dispositivo de rede para se obter todos os serviços TCP e UDP habilitados.
III. Backdoor são sistemas simuladores de servidores que se destinam a enganar um invasor, deixando-o pensar que está invadindo a rede de uma empresa.
IV. Honey Pot é um programa implantado secretamente em um computador com o objetivo de obter informações e dados armazenados, interferir com a operação ou obter controle total do sistema.

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

14) CESPE/2012 - Considerando que, no desenvolvimento de um novo sistema para a empresa, um analista seja encarregado de avaliar e monitorar a utilização de normas e padrões de segurança da informação, julgue o item subsequente:

Caso sejam utilizadas, no novo sistema, assinaturas digitais para a autenticação das correspondências entre os usuários, as mensagens podem ser criptografadas duas vezes: uma com a utilização da chave privada do remetente e, em seguida, com a utilização da chave pública do receptor.

A) VERDADEIRA B) FALSA

15) FCC/2009 - O impedimento do acesso autorizado aos recursos ou o retardamento de operações críticas por um certo período de tempo é um tipo de ataque denominado

a) engenharia social.
b) trojan horse.
c) denial of service.
d) backdoor.
e) rootkit.

16) CESPE/2010 - No que se refere às técnicas de programação utilizando banco de dados, julgue:

A injeção de SQL (SQL injection, relacionada à structured query language - linguagem de consulta estruturada) é uma técnica de injeção de código que explora a vulnerabilidade de segurança da camada de banco de dados de uma aplicação. Quando se consegue inserir uma ou mais instruções SQL dentro de uma consulta, ocorre o fenômeno.

A) CERTA B) ERRADA

17) Uma pesquisa realizada pelos organizadores da Conferência Infosecurity Europe 2003 com trabalhadores de escritórios, que distribuía um brinde (de baixo valor) aos entrevistados, revelou que 75% deles se dispunham a revelar suas senhas em resposta a uma pergunta direta ("Qual é a sua senha?"), e outros 15% responderam a perguntas indiretas que levariam à determinação da senha. Esse experimento evidencia a grande vulnerabilidade dos ambientes computacionais a ataques de

a) engenharia social.
b) acesso físico.
c) back doors.
d) vírus de computador.
e) cavalos de tróia.

18) No que tange à segurança, existem duas classes de algoritmos criptográficos, caracterizadas a seguir.

1- utiliza uma mesma chave tanto para cifrar como para decifrar uma mensagem, ou seja, a mesma chave utilizada para “fechar o cadeado” é utilizada para “abrir o cadeado”.
2- utiliza chaves distintas, uma para cifrar e “fechar” e outra para decifrar e “abrir”, sempre geradas aos pares.

As classes descritas caracterizam algoritmos criptográficos conhecidos, respectivamente, como:
a) absolutos e relativos
b) simétricos e assimétricos
c) de chave pública e de chave secreta
d) de assinatura assimétrica e de assinatura simétrica
e) de cifras de transposição e de cifras de substituição