Segurança da Informação – SIN

Prof. Pedro Carlos da Silva Lara
Instituto Superior de Tecnologia em Ciências da Computação de Petrópolis
Lista de Exercícios 6

Questão 1) Marque como verdadeiro **(V)** ou falso **(F)**.
( ) 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.

( ) 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.

( ) Um spyware consiste em uma falha de segurança intencional, gravada no computador ou no sistema operacional, a fim de permitir a um cracker obter acesso ilegal e controle da máquina.

( ) Honeypots são mecanismos de segurança, geralmente isolados e monitorados, que aparentam conter informação útil e valiosa para a organização. São armadilhas para enganar agentes nvasores como spammers ou crackers.

( ) Não é possível controlar totalmente nem eliminar as ameaças de segurança da informação em uma organização, pois elas são frequentes e muitas vezes imprevisíveis.

( ) Um ataque de SQL injection explora vulnerabilidades presentes em aplicações web, podendo ser evitado com inspeção criteriosa dos dados de entrada.

( ) A técnica de spoofing é normalmente utilizada na fase de invasão a redes de computadores.

( ) Ataques denominados buffer overflows, tanto na heap quanto na stack, levam à execução arbitrária de código, podendo ser evitados pela retirada de privilégios de execução e pela checagem de integridade das estruturas citadas.

Questão 2) [**FCC - 2012 - TST - Analista Judiciário**] Com relação à segurança da informação, assinale a opção correta.

a) Backdoor é um programa que permite o acesso de uma máquina a um invasor de computador, pois assegura a acessibilidade a essa máquina em modo remoto, sem utilizar, novamente, os métodos de realização da invasão.
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) Bot 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.

Questão 3) [**IADES - 2011 - PG-DF - Analista Jurídico**] Um software malicioso explora uma vulnerabilidade ou falha de configuração de um sistema, podendo se propagar automaticamente por meio de uma rede de computadores, sem a necessidade de ser explicitamente executado por um usuário de computador. Este software é denominado

a) Verme (worm).
b) Cavalo de tróia.
c) Hoax.
d) Rookit.
e) Phishing

Questão 4) Vírus de computador e outros programas maliciosos (Malwares) agem de diferentes formas para infectar e provocar danos em computadores. O Malware que age no computador capturando as ações e as informações do usuário é denominado

a) Cavalo de Troia.
b) Keyloggers.
c) Backdoors.
d) Spyware.
e) Worm.

Questão 5) Analise as afirmativas abaixo sobre ataques digitais.

I. Denial of Service é um ataque que visa interromper um serviço por meio de sobrecarga no servidor ou no meio de comunicação associados ao serviço.

II. Spoofng é um tipo de ataque que intercepta pacotes de rede para obter informações como nomes de usuários ou senhas.

III. Worms são programas que se propagam para infectar o ambiente onde eles se encontram.

Assinale a alternativa CORRETA:
a) A afirmativa III está errada e as afirmativas I, II estão corretas.
b) A afirmativa II está errada e as afirmativas I, III estão corretas.
c) A afirmativa I está errada e as afirmativas II, III estão corretas.
d) As afirmativas I, II e III estão corretas.

Questão 6) [**FEPESE - 2010 - SEFAZ-SC**] Assinale a alternativa que indica corretamente dois tipos de aplicativos maliciosos capazes de se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador.
a) Bot e Worm
b) Vírus e Worm
c) Keylogger e Bot
d) Cavalo de Troia (trojan) e Keylogger
e) Cavalo de Troia (trojan) e Vírus

Questão 7) [**FCC - 2010 - TRF**] Infectam arquivos de programas Word, Excel, Power Point e Access, também aparecendo em outros arquivos. São os vírus
a) de mutação.
b) polimórficos.
c) de split.
d) de boot.
e) de macro.

Questão 8) [**CESGRANRIO - 2010 - BACEN**] Um dos crimes que mais causam prejuízos às pessoas e às instituições é a fraude. Utilizando-se da Internet, fraudadores têm enviado e-mails com mensagens que induzem o usuário a fornecer dados pessoais e financeiros. Esse tipo de fraude, que se dá mediante o envio de mensagem não solicitada, supostamente de uma instituição conhecida, como um banco, e que procura induzir o acesso a páginas fraudulentas, projetadas para furtar dados pessoais e financeiros, constitui a prática de

a) spam.
b) phishing.
c) worm.
d) adware.
e) spyware.

Questão 9) [**FCC - 2012 - MPE-AP**] Sobre spyware é correto afirmar:
a) Trojans são programas spyware que parecem ser apenas cartões virtuais animados, álbuns de fotos, jogos ou protetores de tela e que são instalados automaticamente no computador do usuário com o objetivo de obter informações digitadas por meio do teclado físico ou virtual.
b) Adware é um programa spyware projetado especificamente para apresentar propagandas. É usado apenas para fins legítimos, incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos.
c) São softwares exclusivamente de uso malicioso projetados para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Executam ações que podem comprometer a privacidade do usuário e a segurança do computador.
d) Keylogger é um programa spyware capaz de capturar e armazenar as teclas digitadas pelo usuário. Sua ativação não pode ser condicionada a uma ação prévia do usuário, como o acesso a um site de Internet Banking.
e) Screenlogger é um tipo de spyware capaz de armazenar a posição do cursor e a tela apresentada no monitor nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais.

Questão 10) [**FCC - 2012 - MPE-AP**] É um tipo específico de phishing que envolve o redirecionamento da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS (Domain Name System). Neste caso, quando o usuário tenta acessar um site legítimo, o navegador Web é redirecionado, de forma transparente, para uma página falsa.

O tipo de phishing citado no texto é conhecido como

a) advance fee fraud.
b) hoax.
c) pharming.
d) defacement.
e) source spoofing.

Questão 11) [**ESAF - 2012 - CGU**] A ameaça de segurança em que o atacante consegue inserir uma série de instruções SQL dentro de uma consulta (query) através da manipulação da entrada de dados de uma aplicação é conhecida como

a) SQL Mixing.
b) SQL False Query.
c) SQL Fake Query.
d) SQL Query Attack.
e) SQL Injection.

Questão 12) [**FCC - 2012 - MPE-AP**] Sobre o tratamento de incidentes, analise:

I. Propagação de vírus ou outros códigos maliciosos.

II. Ataques de engenharia social.

III. Modificações em um sistema, sem o conhecimento ou consentimento prévio de seu proprietário.

IV. Ocorrência de monitoramento indevido de troca de mensagens.

Constitui exemplos de incidente de segurança que deve ser reportado o que consta em:

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

Questão 13) [**ESAF - 2005 - Receita**] Em relação a vírus de computador é correto afirmar que, entre as categorias de malware, o Cavalo de Tróia é um programa que

a) usa um código desenvolvido com a expressa intenção de se replicar. Um Cavalo de Tróia tenta se alastrar de computador para computador incorporando-se a um programa hospedeiro. Ele pode danificar o hardware, o software ou os dados. Quando o hospedeiro é executado, o código do Cavalo de Tróia também é executado, infectando outros hospedeiros e, às vezes, entregando uma carga adicional.
b) parece útil ou inofensivo, mas que contém códigos ocultos desenvolvidos para explorar ou danificar o sistema no qual é executado. Os cavalos de tróia geralmente chegam aos usuários através de mensagens de e-mail que disfarçam a fialidade e a função do programa. Um Cavalo de Tróia faz isso entregando uma carga ou executando uma tarefa mal-intencionada quando é executado.
c) usa um código mal-intencionado auto-propagável que pode se distribuir automaticamente de um computador para outro através das conexões de rede. Um Cavalo de Tróia pode desempenhar ações nocivas, como consumir recursos da rede ou do sistema local, possivelmente causando um ataque de negação de serviço.
d) pode ser executado e pode se alastrar sem a intervenção do usuário, enquanto alguns variantes desta categoria de malware exigem que os usuários executem diretamente o código do Cavalo de Tróia para que eles se alastrem. Os Cavalos de Tróia também podem entregar uma carga além de se replicarem.
e) não pode ser considerado um vírus ou um verme de computador porque tem a característica especial de se propagar. Entretanto, um Cavalo de Tróia pode ser usado para copiar um vírus ou um verme em um sistema-alvo como parte da carga do ataque, um processo conhecido como descarga. A intenção típica de um Cavalo de Tróia é interromper o trabalho do usuário ou as operações normais do sistema. Por exemplo, o Cavalo de Tróia pode fornecer uma porta dos fundos no sistema para que um hacker roube dados ou altere as definições da configuração.

Questão 14) Em relação às políticas de segurança, o tipo de firewall instalado em servidores, que serve de intermediador, não permitindo a comunicação direta entre a rede e a Internet, também conhecida como proxy, é o firewall:

a) de filtragem de pacotes;
b) anti-spyware;
c) de aplicação;
d) anti-spam;
e) DMZ.

Questão 15) [**FCC - 2010 - TCE-SP**] Quanto à segurança da informação, é correto afirmar:

a) Buffer Overflow é um ataque que pode ser realizado para sobrecarregar o poder de resposta de um servidor em um sistema de informação.
b) Vírus de macro é um programa malicioso que vasculha um computador secretamente capturando e gravando todas as digitações, acessos aos websites visitados, quando acessados a partir de arquivos com extensão .doc.
c) Inutilizar, mesmo que momentaneamente, um sistema de informação, incapacitando seu servidor de responder às requisições feitas pelos clientes, é o objetivo do ataque DoS (Denial of Sevice).
d) Exigir identificação dos remetentes das mensagens que chegam, bem como autenticar as assinaturas digitais das mensagens de correio a serem enviadas, é tarefa que pode ser realizada por um firewall.
e) Dominar o sistema do usuário para ser manipulado por uma entidade externa é o objetivo do virus Spyware.

Questão 16) [**FCC - 2011 - TRE-RN**] Considere:

I. Tipo de ataque onde é enviada uma enorme quantidade de pedidos a um determinado serviço a fim de sobrecarregá-lo e deixá-lo inoperante.

II. Sistema instalado na rede que analisa todos os pacotes e tenta detectar os ataques definidos em (I).

I e II são, respectivamente,

a) NIDS e QoS.
b) IDS e DoS.
c) PIDS e HIDS.
d) DoS e NIDS.
e) QoS e IDS.

Questão 17) [**FGV - 2010 - BADESC**] O Firewall do Windows representa uma barreira de proteção que monitora os dados transmitidos entre um computador e a Internet, fornecendo uma defesa contra pessoas que busquem o acesso sem permissão, a partir de um computador de fora desse firewall.

Além de ajudar no bloqueio de vírus, são atividades executadas pelo Firewall do Windows:

a) detectar e desativar vírus e solicitar permissão para bloquear ou desbloquear determinados pedidos de conexão.
b) solicitar permissão para bloquear ou desbloquear determinados pedidos de conexão e criar um log de segurança.
c) criar um log de segurança e impedir a abertura de e-mails com anexos perigosos.
d) impedir a abertura de e-mails com anexos perigosos e bloquear spam ou e-mail não solicitado.
e) bloquear spam ou e-mail não solicitado e detectar e desativar vírus.

Questão 18) Um firewall, tanto físico quanto lógico, tem por finalidade evitar a invasão e a utilização de uma rede e de seus servidores e estações de trabalho por softwares ou pessoas não autorizadas. A configuração de um firewall consiste em uma

a) combinação de regras que abrem ou fecham as portas lógicas e nas regras de verificação de protocolos TCP/IP e UDP.
b) criação de rede com cabeamento estruturado intercalada por roteadores e switchs.
c) implementação da lista de regras administrativas com as permissões de uso da rede pelos usuários.
d) instalação de pacotes com atualizações de segurança fornecidas pelo fabricante do sistema operacional dos servidores de rede.
e) permissão ou um bloqueio do acesso a URLs determinadas pelo gestor de segurança.

Questão 19) [**FCC - 2009 - TJ-PA**] Os proxies instalados em computadores servidores que não permitem a comunicação direta entre uma rede e a Internet são firewalls de

a) comunicação.
b) pacotes.
c) filtragem.
d) aplicação.
e) stateful inspection.

Questão 20) [**ESAF - 2010 - SUSEP**] Um dos objetivos do firewall é

a) restringir acesso a ambientes controlados.
b) criar pontos controlados por autorizações informais.
c) restringir a implantação de defesas em ambientes críticos.
d) impedir que haja acesso por um ponto controlado, tendo autorização para tanto.
e) impedir que eventuais atacantes cheguem muito perto das ameaças desconhecidas.

Questão 21) [**ESAF - 2009 - ANA**] O mecanismo de controle de acesso adequado para bloquear segmentos UDP e conexões FTP, em uma rede, é o(a)

a) sistema de detecção de intrusos (SDI).
b) firewall de filtragem de pacotes.
c) rede privada virtual (VPN).
d) gateway de aplicação.
e) rede local virtual (VLAN).

Questão 22) São exemplos, respectivamente, de um Firewall e de um sistema de detecção de intrusão:
a) Nmap e Snort
b) Kerberos e NMap
c) IPTables e Snort
d) IPTables e Kerberos
e) Snort e PortKnocking

Questão 23) [**ESAF - 2006 - CGU**] A proteção dos sistemas utilizados pelos fornecedores de serviços pela Internet requer a aplicação de ferramentas e conceitos de segurança eficientes. Quanto ao firewall que trabalha na filtragem de pacotes, um dos mais importantes itens de segurança para esses casos, é correto afirmar que ele

a) se restringe a trabalhar nas camadas HTTP, decidindo quais pacotes de dados podem passar e quais não. Tais escolhas são regras baseadas nas informações do serviço remoto, endereço IP do destinatário, além da porta UDP usada.
b) é capaz de controlar conexões pelas portas UDP utilizadas, além de ser capaz de analisar informações sobre uma conexão já estabelecida, sem o uso de portas.
c) é instalado geralmente em computadores servidores, também conhecidos como proxy.

d) determina que endereços IPs podem estabelecer comunicação e/ou transmitir ou receber dados.
e) além de ter a capacidade de analisar o conteúdo dos pacotes, o que permite um controle ainda maior, pode ou não ser acessível para conexões que usam porta UDP.

Questão 24) [**FCC - 2012 - TCE-SP**] O termo insegurança computacional está relacionado, entre outras coisas, a ação de programas que podem comprometer a segurança dos recursos e informações contidas em ambientes computacionais. Sobre esses programas, considere:

I. É um código escrito com a intenção explícita de se autoduplicar. Tenta se alastrar de computador para computador, incorporando-se a um programa hospedeiro. Ele pode danificar hardware, software ou informações.

II. Cria cópias de si mesmo de um computador para outro automaticamente, ou seja, sem a ação do usuário. Primeiro ele controla recursos no computador que permitem o transporte de arquivos ou informações. Depois que ele contamina o sistema, ele se desloca sozinho, distribuindo cópias de si mesmo pelas redes. Seu grande perigo é a capacidade de se replicar em grande volume. Não precisa de um programa hospedeiro.

III. É um programa de computador que parece ser útil, mas na verdade causa danos. Alastra-se quando a pessoa é seduzida a abrir um programa por pensar que ele vem de uma fonte legítima.

IV. É um termo genérico usado para softwares que realizam certas atividades como anúncios, coleta de informações pessoais ou alteração das configurações do computador, geralmente sem o devido consentimento.

Os itens I, II, III e IV referem-se, correta e respectivamente, a

a) worm, phishing, vírus, spyware.
b) vírus, worm, cavalo de Troia e spyware.
c) cavalo de Troia, vírus, worm e phishing.
d) vírus, spyware, worm e adware.
e) worm, vírus, spyware e spam.

Questão 25) [**FCC - 2012 - TJ-RJ**] 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) port scanning.
b) backdoor.
c) cookie hijacking.
d) denial of service.
e) phishing.

Questão 26) [**ESAF - 2004 - CGU**] Analise as seguintes afirmações relativas a um firewall:

I. Um firewall é um equipamento, ou conjunto de equipamentos, cujo objetivo é controlar o tráfego entre redes.

II. Um firewall, quando configurado corretamente, deve impedir invasões que partam de máquinas na rede em que se encontra a máquina alvo da invasão.

III. Em um firewall, os filtros definem valores que os cabeçalhos dos pacotes devem apresentar de forma que possam ser filtrados em função de critérios como tipo de protocolo e endereço e porta de origem e destino.

IV. De uma forma geral, um firewall não pode ser instalado em um roteador porque as características de seus filtros impedem o correto roteamento dos pacotes, o que transformaria o roteador em um simples Hub.

Estão corretos os itens:

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

Questão 27) [**IADES - 2011 - PG-DF**] Em situação hipotética, um órgão de segurança do governo está sofrendo um ataque ao seu servidor web. O perito em segurança, responsável por analisar o incidente, tomou a decisão de investigar a ação criminosa em andamento, com o objetivo de estudar o seu comportamento e obter informações sobre as técnicas de ataques utilizadas. Assinale a alternativa adequada a esse tipo de análise.

a) Firewall
b) Botnet.
c) DMZ.
d) Hijacking.
e) Honeypot.

Questão 28) [**FCC - 2011 - TRT**] No caso de phishing, no qual o atacante comprometeu o servidor de nomes do provedor (DNS), de modo que todos os acessos a determinados sites passaram a ser redirecionados para páginas falsificadas, a ação que, preventivamente, se apresenta mais adequada é

a) verificar a autenticidade do certificado digital.
b) digitar novamente o endereço diretamente no browser e compará-lo com a página anterior.
c) observar o endereço apresentado na barra de status do browser e verificar se ele corresponde ao do site pretendido.

d) verificar o endereço IP do provedor de Internet visitado.
e) utilizar comandos, tais como ping e telnet, para verificar a confiabilidade do site.

Questão 29) [**FCC - 2009 - TCE-GO**] Considere a hipótese de recebimento de uma mensagem não solicitada de um site popular que induza o recebedor a acessar uma página fraudulenta projetada para o furto dos dados pessoais e financeiros dele. Trata-se de

a) spam.
b) phishing/scam.
c) adware.
d) keylogger.
e) bluetooth.

Questão 30) [**FCC - 2009 - TCE-GO**] 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) Social Engineering.
b) Sniffer.
c) Service Set Identifier.
d) Exploit.
e) Denial of Service.

Questão 31) [**FCC - 2009 - TCE-GO**] É um tipo de ataque passivo às transmissões de dados por meio de redes de computadores o de

a) falsidade.
b) negação de serviço.
c) análise de tráfego.
d) repetição.
e) modificação de mensagem.

Questão 32) É um aplicativo usado tanto pelas áreas de segurança, para análise de vulnerabilidades, quanto por pessoas mal intencionadas, para identificarem portas abertas e planejarem invasões:
a) Denial of Service.
b) Port Scan.
c) Buffer Overflow.
d) DNS Spoofing.
e) Brute Force Attack.

Questão 33) [**FEPESE - 2010 - SEFAZ-SC**] Em relação aos crimes eletrônicos e aos fundamentos da investigação criminal, julgue as afirmativas abaixo.

1. Os crimes digitais envolvem as condutas criminosas cometidas com o uso das tecnologias de informação e comunicação e aquelas nos quais o objeto da ação criminosa é o próprio sistema informático.
2. Os delitos informáticos próprios são aqueles praticados diretamente pelo agente, sem a participação de nenhum outro indivíduo.
3. Em razão do princípio da tipicidade penal, enquanto não for aprovada a lei de crimes digitais, ninguém pode ser condenado por prática de atividades ilícitas através da Internet.
4. Pode ser considerado um delito informático impróprio o crime de estelionato praticado, dentre outros artifícios, através da técnica de phishing.
5. Enquanto não for expressamente prevista em lei, a difusão de código malicioso, sem que haja a comprovação de dano, não pode ser considerada como crime.

Assinale a alternativa que indica todas as afirmativas corretas.

a) São corretas apenas as afirmativas 1 e 4.
b) São corretas apenas as afirmativas 2 e 5.
c) São corretas apenas as afirmativas 3 e 5.
d) São corretas apenas as afirmativas 1, 2 e 3.
e) São corretas apenas as afirmativas 1, 4 e 5.

Questão 34) [**CESGRANRIO - 2010 - ELETROBRÁS**] 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.

Questão 35) [**FCC - 2008 - TCE-AL**] No âmbito das possibilidades de invasão de redes de computadores, SNORT é

a) um agente de comunicação de invasão adotado pelo SMTP.
b) um protocolo de defesa situado na camada de enlace OSI.
c) uma ferramenta NIDS open-source.
d) um modelo de criptografia antiinvasão.
e) um padrão IDS de configuração de portas de segurança.