



SEGURANÇA, POLÍTICA DE SEGURANÇA E BACKUP – ESAF

01 - **(ESAF - Auditor-Fiscal da Previdência Social - AFPS - 2002)** Os problemas de segurança e crimes por computador são de especial importância para os projetistas e usuários de sistemas de informação. Com relação à segurança da informação, é correto afirmar que

- a) confiabilidade é a garantia de que as informações armazenadas ou transmitidas não sejam alteradas.
- b) integridade é a garantia de que os sistemas estarão disponíveis quando necessários.
- c) confiabilidade é a capacidade de conhecer as identidades das partes na comunicação.
- d) autenticidade é a garantia de que os sistemas desempenharão seu papel com eficácia em um nível de qualidade aceitável.
- e) privacidade é a capacidade de controlar quem vê as informações e sob quais condições.

02 - **(ESAF - Auditor-Fiscal da Previdência Social - AFPS - 2002)** Uma informação, para ser considerada segura, precisa manter seus aspectos de confiabilidade, integridade e disponibilidade.

A confiabilidade é a

- a) propriedade de evitar a negativa de autoria de transações por parte do usuário, garantindo ao destinatário o dado sobre a autoria da informação recebida.
- b) garantia de que o sistema se comporta como esperado, em geral após atualizações e retificações de erro.
- c) análise e responsabilização de erros de usuários autorizados do sistema.
- d) garantia de que as informações não poderão ser acessadas por pessoas não autorizadas.
- e) propriedade que garante o acesso às informações através dos sistemas oferecidos.

03 - **(ESAF - Auditor-Fiscal da Previdência Social - AFPS - 2002)** Em um sistema em segurança de redes de computadores, a intrusão é qualquer conjunto de ações que tendem a comprometer a integridade, confidencialidade ou disponibilidade dos dados ou sistemas.

Com relação aos sistemas de detecção de intrusos – IDS, é correto afirmar que, na tecnologia de detecção de intrusos Host Based,

- a) os IDSs são instalados em várias máquinas que serão responsáveis por identificar ataques direcionados a toda a rede.
- b) o IDS é instalado em um servidor para alertar e identificar ataques e tentativas de acessos indevidos à própria máquina.
- c) o IDS é instalado em uma máquina que analisa todos os dados que transitam na rede segundo um conjunto de regras específicas.
- d) o IDS funciona de forma passiva em diferentes ambientes, não interferindo no desempenho da máquina na qual está instalado.
- e) o IDS é instalado em uma máquina que analisa todos os dados que transitam na rede para identificar a assinatura dos dados capturados.

04 - **(ESAF - Auditor-Fiscal do Trabalho - MTE - 2003)** O Ping da Morte (Ping of Death) é um recurso utilizado na Internet por pessoas mal intencionadas, que consiste

- a) no envio de pacotes TCP/IP de tamanho inválidos para servidores, levando-os ao travamento ou ao impedimento de trabalho.
- b) na impossibilidade de identificação do número de IP de máquina conectada à rede. Desta forma, muitos dos serviços de segurança disponíveis deixam de funcionar, incluindo os "rastreamentos" que permitem a identificação de segurança das fontes de origem de ataques.
- c) em instalar em um computador conectado a uma rede um programa cliente que permite a um programa servidor utilizar esta máquina sem restrições.
- d) no mecanismo de "abertura" de portas e acha-se atualmente incorporado em diversos ataques de vírus.
- e) na captura e alteração de "pacotes" TCP/IP transmitidos pelas redes.

05 - **(ESAF - Auditor-Fiscal do Trabalho - MTE - 2003)** A manutenção da segurança da informação e serviços de tecnologia da informação é responsabilidade dos profissionais de suporte e auditores de sistemas, que têm como prioridade de suas ações a garantia de funcionamento de sistemas da informação. Com relação à segurança da informação, é correto afirmar que

- a) apenas o tráfego autorizado, tal como definido pela política de segurança da empresa, deve ser permitido chegar ao Firewall.
- b) um Firewall, quando configurado de forma a "o que não for explicitamente proibido, é permitido", impede o sucesso de novos ataques que utilizam tecnologias ou métodos até então desconhecidos.
- c) um Firewall, quando configurado corretamente, promove a segurança de uma rede controlando o tráfego baseado em origem e destino, desconsiderando o protocolo utilizado pelo pacote protocolo.
- d) um Firewall é um sistema que permite o controle de tráfego entre duas ou mais redes.
- e) um Firewall, quando configurado corretamente, não consegue realizar conversão de endereço via NAT

06 - **(ESAF - Auditor-Fiscal da Receita Federal do Brasil - AFRFB - 2005)** Analise as seguintes afirmações relacionadas aos conceitos básicos de Segurança da Informação:

- I. O IP spoofing é uma técnica na qual o endereço real do atacante é mascarado, de forma a evitar que ele seja encontrado. É normalmente utilizada em ataques a sistemas que utilizam endereços IP como base para autenticação.
- II. O NAT, componente mais eficaz para se estabelecer a segurança em uma rede, é uma rede auxiliar que fica entre a rede interna, que deve ser protegida, e a rede externa, normalmente a Internet, fonte de ataques.
- III. O SYN flooding é um ataque do tipo DoS, que consiste em explorar mecanismos de conexões TCP, prejudicando as conexões de usuários legítimos.
- IV. Os Bastion host são equipamentos que atuam com proxies ou gateways entre duas redes, permitindo que as requisições de usuários externos cheguem à rede interna.

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

07 - **(ESAF - Auditor-Fiscal da Receita Federal do Brasil - AFRFB - 2005)** Analise as seguintes afirmações relacionadas à segurança na Internet:

- I. Um IDS é um sistema de segurança que tem como principal objetivo bloquear todo o tráfego, que utilize o protocolo http, aos servidores WWW de uma corporação.
- II. Uma VPN é formada pelo conjunto de tunelamento que permite a utilização de uma rede pública para o tráfego de informações e, com o auxílio da criptografia, permite um bom nível de segurança para as informações que trafegam por essa conexão.
- III. Configurando um firewall, instalado entre uma rede interna e a Internet, para bloquear todo o tráfego para os protocolos HTTP, SMTP, POP e POP3, os usuários da referida rede interna terão acesso à Internet, com um nível de segurança aceitável, a sites como os de bancos, servidores de e-mail e de entidades que utilizem sites seguros.
- IV. O firewall é um programa que tem como objetivo proteger uma rede contra acessos e tráfego indesejado, proteger serviços e bloquear a passagem de conexões indesejáveis, como por exemplo, aquelas vindas da Internet com o objetivo de acessar dados corporativos ou seus dados pessoais.

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

08 - **(ESAF - Auditor-Fiscal da Receita Federal do Brasil - AFRFB - 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

09 - **(ESAF - Ministério do Planejamento, Orçamento e Gestão - 2006)** Quanto aos conceitos básicos de Segurança da Informação é correto afirmar que Autenticação é o processo

- a) que rastreia as atividades dos usuários ao gravar tipos selecionados de eventos no log de segurança de um servidor ou de uma estação de trabalho.
- b) iniciado para impedir que usuários acessem um serviço de rede, como um servidor Web ou um servidor de arquivos.
- c) que disponibiliza a lista de programas do menu Iniciar para todos os usuários do Windows que fazem login no computador.
- d) de transmissão de mensagens que permite que um aplicativo distribuído possa acessar serviços disponíveis em vários computadores em uma rede.
- e) utilizado para verificar se uma entidade ou objeto é quem ou o que afirma ser.

10 - **(ESAF - Técnico da Receita Federal - TRF - 2005)** Nos dispositivos de armazenamento de dados, quando se utiliza espelhamento visando a um sistema tolerante a falhas, é correto afirmar que

- a) ao apagar um arquivo em um disco com sistema de espelhamento, o arquivo equivalente no disco espelhado só será apagado após a execução de uma ação específica de limpeza que deve ser executada periodicamente pelo usuário.
- b) ao ocorrer uma falha física em um dos discos, os dados nos dois discos tornam-se indisponíveis. Os dados só serão mantidos em um dos discos quando se tratar de uma falha de gravação de dados.
- c) o sistema fornece redundância de dados usando uma cópia do volume para duplicar as informações nele contidas.
- d) o disco principal e o seu espelho devem estar sempre em partições diferentes, porém no mesmo disco físico.
- e) o disco a ser utilizado como espelho deve ter sempre o dobro do tamanho do disco principal a ser espelhado.

11 - **(ESAF - Técnico da Receita Federal - TRF - 2005)** Analise as seguintes afirmações relacionadas a vírus e antivírus.

- I. Um cookie é um vírus do tipo malware que pode ser armazenado pelo browser se um website requisitar. A informação não tem um tamanho muito grande e, quando acionados, alteram a configuração de segurança do browser.
- II. Qualquer malware que possua um backdoor permite que o computador infectado seja controlado totalmente ou parcialmente através de um canal de IRC ou via conexão com uma porta.
- III. O Cavalo de Tróia é um programa que, explorando deficiências de segurança de computadores, propaga-se de forma autônoma, contaminando diversos computadores geralmente conectados em rede. O Cavalo de Tróia mais conhecido atacou quantidades imensas de computadores na Internet durante os anos 90.
- IV. A Engenharia Reversa é a arte de reverter códigos já compilados para uma forma que seja legível pelo ser humano. Técnicas de engenharia reversa são aplicadas na análise de vírus e também em atividades ilegais, como a quebra de proteção anticópia. A engenharia reversa é ilegal em diversos países, a não ser que seja por uma justa causa como a análise de um malware.

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

12 - **(ESAF - Técnico da Receita Federal - TRF - 2005)** Entre as técnicas utilizadas pelos hackers, a sniffing consiste

- a) no envio de um SYN como se fosse abrir uma conexão real que, em seguida, envia outro SYN para o fechamento da conexão. Este método é utilizado para interrupção de todas as conexões estabelecidas pelo sistema.
- b) na abertura de uma conexão TCP em uma porta alvo.
- c) na abertura de uma conexão UDP em uma porta alvo.
- d) na captura de pacotes que trafegam no mesmo segmento de rede em que o software funciona.
- e) na utilização de ferramentas para fazer o mapeamento de portas TCP e UDP acessíveis.

GABARITO

01 - E 02 - D 03 - B 04 - A 05 - D 06 - D 07 - E
08 - A 09 - E 10 - C 11 - E 12 - D