



1 - Analise os itens e aponte a opção incorreta:

I. Em segurança da informação, de acordo com o princípio da confidencialidade, somente o remetente e o destinatário pretendido podem entender o conteúdo da mensagem transmitida.

II. A integridade da mensagem é desejável em uma comunicação segura. Neste princípio, devemos garantir que o conteúdo de sua comunicação não seja alterado durante a transmissão.

III. Um dos princípios básicos da segurança da informação é a disponibilidade. Neste princípio, devemos garantir que os usuários são quem eles realmente dizem ser.

IV. Em criptografia, a função de uma chave criptográfica é personalizar o processo de criptografia, uma vez que o processo a ser realizado utilizará a combinação do algoritmo desejado com a chave informada pelo usuário.

- a) I e III, somente;
- b) II, somente;
- c) II e III, somente;
- d) III somente;
- e) IV, somente.

2 - A detecção instantânea da intrusão em uma rede de computadores é um dos aspectos primordiais para a segurança da informação. Para tal, existem diversas ferramentas, como o IDS (Intrusion Detection System) de rede que pode realizar a detecção por meio da monitoração

- a) da quantidade de usuários do sistema operacional.
- b) do estado da placa de rede do computador.
- c) de pacotes com aplicativos nocivos.
- d) de pacotes de dados com vírus.
- e) de varreduras de Portas TCP.

3 - O armazenamento de cópias de segurança de grandes volumes de dados, de maior importância, que devem perdurar por longos períodos, são critérios determinantes para maiores cuidados, principalmente, com

- a) os dados escolhidos para gravação e guarda.
- b) a qualidade e a confiança nas mídias usadas.
- c) a restrição de acesso ao local de armazenamento.
- d) a guarda de cópias em locais diferentes.
- e) a criptografia dos dados gravados.

4 - Ataques de negação de serviços DoS fazem com que recursos sejam explorados de maneira agressiva, de modo que usuários legítimos ficam impossibilitados de utilizá-los. Uma técnica típica causa o overflow da pilha de memória, por meio do

envio de um grande número de pedidos de conexão, que não podem ser completados ou manipulados. Essa técnica é conhecida por

- a) IP Fragmentation
- b) Smurf Scanning.
- c) Packet Sniffing.
- d) SYN Flooding
- e) Negação de pacotes

5 - Uma empresa tomou as seguintes medidas:

- As configurações de sistemas passaram a ser guardadas separadamente;

- A execução dos procedimentos passou a ser periódica e com agendamentos a serem seguidos rigorosamente;

- O acesso físico aos dados copiados passou a ser protegido contra destruição física e contra acessos não autorizados;

- Os privilégios de execução dos procedimentos e de recuperação (restore) dos dados foram redefinidos;

- Os testes dos dados copiados passaram a ser feitos periodicamente para verificar se continuam utilizáveis, ou seja, se não se deterioraram;

- Os dados copiados passaram a ser armazenados em dois locais diferentes: um no local próximo ao equipamento e outro num local físico protegido e diferente do original. Essa medida irá garantir que, caso haja uma catástrofe, ainda será possível conseguir recuperar os dados.

Estas medidas estão relacionadas a procedimentos de

- a) Administração de usuários.
- b) Controle de acessos.
- c) Separação de ambientes: produção, desenvolvimento e testes.
- d) Cópias de segurança: backup.
- e) Segurança de dados na rede.

6 - É um dispositivo que não só examina os cabeçalhos de todos os pacotes que passam por ele, mas também executa uma inspeção profunda de pacote. Quando tal dispositivo observa o pacote suspeito, ou uma série de pacotes suspeitos, ele envia um alerta ao administrador da rede que pode examinar o tráfego minuciosamente e tomar as ações necessárias.



@EXPLICADORES.NET

WWW.EXPLICADORES.NET.BR



O dispositivo citado acima é conhecido como

- a) IPS.
- b) IDS.
- c) Firewall de filtragem de pacotes.
- d) SSL.
- e) DMZ.

7 - Os IPSs:

- a) possuem altas taxas de falso-positivas e por esse motivo não permitem detectar ataques de negação de serviço.
- b) permitem alertar uma tentativa de ataque, mas não realizar o seu bloqueio.
- c) possuem equipamentos que normalmente trabalham na camada de aplicação do modelo OSI (camada 7) e necessitam de reconfiguração da rede para serem instalados.
- d) permitem detectar a propagação de vírus, worms, ataques a sistemas operacionais e à Web, mas não permitem detectar spams, phishing e spyware.
- e) realizam um nível de inspeção no pacote muito profundo, que vai até a camada de aplicação do modelo OSI (camada 7).

8 - Sobre DDoS, assinale a alternativa correta.

- a) É uma forma de ataque repetitivo a um determinado endereço, visando descobrir através de algoritmos o login e senha de um determinado serviço em um servidor em questão.
- b) DDoS é quando temos um software intruso dentro de nosso servidor, esse software faz ataque a outros servidores sem nossa autorização.
- c) Esse ataque é classificado quando um intruso tem sob seu comando centenas de computadores, e comanda um ataque ao mesmo alvo e ao mesmo instante.
- d) DDoS é um protocolo responsável para envio e recebimento de e-mails.
- e) DDoS é o nome dado ao Firewall mais utilizado em servidor Red Hat Enterprise Linux 6.

9 - O ataque do tipo negação de serviços (DoS ou DDoS) tem o objetivo de

- a) tirar de operação um ou mais serviços ou computadores conectados à Internet.
- b) invadir computadores para roubar informações sigilosas.
- c) quebrar senhas de acesso para bisbilhotar sistemas corporativos.

- d) destruir arquivos gravados nos discos magnéticos dos computadores invadidos.
- e) quebrar a criptografia de dados cifrados que transitam nas redes.

10 - Em um sistema de detecção de intrusos, o responsável por analisar todos os pacotes e tentar detectar os ataques do tipo DoS (denial of service), varredura de portas e outras tentativas de ataque é o:

- a) SHA-1.
- b) HIDS.
- c) NIDS.
- d) NAS.
- e) AES.

11 - Análise de comportamento de redes, ou NBA, da sigla, em inglês, Network Behavior Analysis, é uma técnica que examina o tráfego da rede em busca de ameaças que geram fluxos não usuais, como DDoS e violações de políticas da empresa ou um sistema cliente provendo serviços de rede para outros sistemas. Essa técnica de análise é uma característica

- a) dos sistemas IDS e IPS.
- b) do sistema firewall.
- c) do sistema antivírus.
- d) do sistema NAT.
- e) do sistema VPN.

12 - Analise as seguintes afirmativas sobre segurança digital em redes e segurança da informação.

- I. Uma política de segurança é um mecanismo de proteção a partir do momento que é amplamente divulgada e conhecida por todos os funcionários e colaboradores da organização.
- II. Um ataque do tipo DDOS (distributed denial of service) afeta diretamente o fundamento de segurança da informação que trata da disponibilidade.
- III. Uma assinatura digital está diretamente relacionada a identificação biométrica que permite que características físicas sejam utilizadas para garantir a autenticidade de um documento ou para permitir o acesso físico ou lógico a um local ou sistema.

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.
- e) Todas estão erradas.





13 - Sobre segurança em redes sem fio,

- a) a única maneira de detectar falsos concentradores é avaliando a que distância se encontram em relação à estação de monitoramento.
- b) os concentradores podem ser úteis para prover monitoramento do tráfego, o que é suficiente para identificar qualquer tipo de ataque.
- c) o correto monitoramento do ambiente de rede é uma das ações de segurança mais importantes e deve ter prioridade sobre os demais processos de segurança.
- d) o monitoramento de rede pode detectar os pontos de falha, mas não poderão explicar como um determinado ataque, bem sucedido ou não, ocorreu.
- e) o administrador deve monitorar apenas os padrões em uso no ambiente.

14 - Sobre os rootkits é correto afirmar:

- a) O nome rootkit indica que as ferramentas que o compõem são usadas exclusivamente para obter acesso privilegiado (root ou Administrator) em um computador.
- b) Podem fornecer sniffers, para capturar informações na rede onde o computador está localizado, como, por exemplo, senhas que estejam trafegando em claro, ou seja, sem qualquer método de criptografia.
- c) Pode fornecer programas com as mais diversas funcionalidades, exceto backdoors que servem para assegurar o acesso futuro do invasor ao computador comprometido.
- d) São projetados para ficarem visíveis juntamente com uma aplicação conhecida. Sua identificação é sempre uma tarefa bem fácil.
- e) São um softwares construídos exclusivamente para capturar e armazenar as teclas digitadas pelo usuário. Dentre as informações capturadas podem estar senhas bancárias, números de cartões de crédito etc.

15 - Em um ambiente de acesso à Internet, constituem medidas mais adequadas para minimizar os problemas de segurança e produtividade e riscos de contaminação por vírus, trojans e outros códigos maliciosos:

- a) Utilizar filtros para inspeção de conteúdos maliciosos nos acessos à Web.
- b) Adotar políticas de acesso e log para e-mails recebidos/enviados.
- c) Manter atualizadas as ferramentas de antivírus nas estações de trabalho.
- d) Adotar políticas de segurança, ferramentas antivírus e filtro de inspeção de conteúdo em e-mail e acessos a Web.
- e) Implementar antivírus e ferramenta anti-spam.

16 - O usuário do computador recebe uma mensagem não solicitada, geralmente de conteúdo alarmista, a fim de assustá-lo e convencê-lo a continuar a corrente interminável de e-mails para gerar congestionamento na rede. Trata-se de um ataque denominado

- a) Hoax.
- b) Worms.
- c) Trojans.
- d) Spam.
- e) Backdoors.

17 - Em relação às vulnerabilidades de uma rede de computadores, considere:

I. Os HUBs Ethernet são equipamentos que repetem todos os pacotes de rede recebidos em todas as suas portas, o que se constitui num fator de vulnerabilidade, pois, se qualquer computador ou equipamento for invadido, um sniffer pode ser instalado para monitorar todo o tráfego da rede e capturar senhas de acesso aos servidores, além de outras consequências.

II. O armazenamento local dos logs nos servidores pode facilitar a obtenção de informações a respeito das atividades do invasor e, dessa forma, agilizar a implementação de medidas de segurança.

III. O roteador é o ponto de entrada da rede e, apesar dele possuir algumas regras de acesso configuradas, um firewall poderia oferecer uma proteção bem maior.

Está correto o que se afirma, SOMENTE, em:

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

18 - Um tipo de ataque que envolve personagens, tais como, Master (máquina que recebe os parâmetros para o ataque e comanda os agentes) e Agentes (máquinas que efetivamente concretizam o ataque contra uma ou mais vítimas), que inundam os servidores alvo com um volume enorme de pacotes é denominado

- a) Flooding.
- b) DDoS.
- c) Buffer Overflow.
- d) Spoofing.
- e) Sniffers.

19 - Em relação à segurança em redes de computadores existem ataques de negação de serviços, onde o acesso a um sistema é interrompido ou impedido, deixando de



# PROJETO EXPLICADORES.NET



estar disponível; ou uma aplicação, cujo tempo de execução é crítico, é atrasada ou abortada. Trata-se de um ataque que compromete o aspecto da

- a) integridade.
- b) interoperabilidade.
- c) autenticidade.
- d) confidencialidade.
- e) disponibilidade.

20 - Interceptação e Análise de Tráfego são ataques passivos à segurança. Para se defender contra esses tipos de ataque deve-se realizar a

- a) configuração de firewall e DMZ (zona desmilitarizada).
- b) configuração e aplicação de filtros no servidor.
- c) autenticação, e garantir a integridade das informações através de certificação digital e criptografia (assinatura digital).
- d) codificação (criptografia) dos dados, evitando que o seu conteúdo se torne disponível mesmo se interceptado.
- e) aplicação de segurança física dos recursos de processamento e comunicação de dados.

21 - Uma ferramenta utilizada por hackers para capturar dados digitados pelas vítimas é um software analisador de tráfego, que inspeciona pacotes de dados que circulam pela rede e extrai informações deles. Esse programa é conhecido por:

- a) trojan
- b) sniffer
- c) cookie
- d) spoofing
- e) phishing

22 - Uma grande preocupação dos usuários de rede sem fio é com a segurança dos dados trafegados entre o dispositivo móvel e o ponto de acesso da rede. Em relação à configuração de redes sem fio com segurança, qual afirmativa está INCORRETA?

- a) Criptografia com WPA-2 Enterprise necessita de um servidor Radius na rede para autenticação do usuário.
- b) Criptografia WPA-2 PSK não é recomendada para soluções residenciais.
- c) Criptografia WEP é considerada fraca para padrões atuais de segurança.
- d) Criptografia WPA é uma evolução do protocolo de criptografia WEP.

23 - Não faz parte de uma arquitetura básica de segurança para web:

- a) antivírus.
- b) firewall de Aplicação.
- c) criptografia SSL.
- d) firewall IDS/IPS.
- e) escalonamento de tempo.

24 - Em redes de computadores, é o tipo de ataque em que o espião intercepta a comunicação entre dois usuários, de forma que o usuário A comunique-se com ele mesmo pensando ser o usuário B, e o usuário B também o faz, pensando ser o usuário A. Trata-se de

- a) SYN Flooding.
- b) Pharming.
- c) Man-in-The-Middle.
- d) DoS.
- e) Spoofing.

25 - Com relação à robustez do método criptográfico utilizado, a ordem do protocolo mais vulnerável para o menos vulnerável é

- a) TKIP, WPA e WEP.
- b) WPA, TKIP e WEP.
- c) TKIP, WEP e WPA.
- d) WEP, TKIP e WPA ---
- e) WEP, WPA e TKIP.

26 - Considere:

I. Sistema instalado na rede e que analisa todos os pacotes, bem como tenta detectar ataques do tipo DoS, varredura de portas e tentativa de ataques.

II. Sistema que conhece a fundo um determinado protocolo e analisa o tráfego desse protocolo.

III. Sistema que analisa o comportamento interno de uma máquina a fim de detectar qualquer anomalia.

No contexto do IDS, I, II e III correspondem, respectivamente, a

- a) PIDS, HIDS e NIDS.
- b) PIDS, NIDS e HIDS.
- c) NIDS, HIDS e PIDS.
- d) NIDS, PIDS e HIDS.
- e) HIDS, PIDS e NIDS.

27 - A rede delimitadora que tem como objetivo principal segregar o ambiente interno (seguro) do ambiente externo (inseguro), é conhecida como:

- a) backbone.
- b) tcp/ip.
- c) zona desmilitarizada (DMZ).
- d) wi-fi.



e) pki.

28 - Muitos navegadores oferecem ao usuário a opção de bloquear cookies. Tais cookies consistem em

- a) informação de roteamento enviada pelo servidor, com o objetivo de otimizar o tempo de resposta no próximo acesso ao mesmo servidor.
- b) trechos de código que são enviados ao computador do usuário, para serem executados no próximo acesso ao mesmo servidor.
- c) trechos de código da página acessada, que são executados durante o período em que o navegador exibe a página.
- d) informação enviada pelo servidor que hospeda a página, para ser reenviada pelo navegador no próximo acesso ao mesmo servidor. --
- e) informação referente ao computador onde é executado o navegador, que é enviada ao servidor.

29 - São propriedades da comunicação segura:

- a) comodidade, autenticação do ponto final, integridade de mensagem e qualidade operacional.
- b) confidencialidade, autenticação do ponto inicial, integridade de usuário e segurança operacional.
- c) compatibilidade, autenticação do ponto final, integridade de mensagem e qualidade da criptografia.
- d) confidencialidade, autenticação do ponto final, integridade de mensagem e segurança operacional.
- e) confiabilidade, autenticação do ponto de acesso, conteúdo de mensagem e segurança estratégica.

30 - São, respectivamente, um tipo de ataque de segurança passivo e um ativo às redes de computadores:

- a) falsidade e modificação de mensagens.
- b) análise de tráfego e vazamento de conteúdo de mensagens.
- c) falsidade e negação de serviço.
- d) análise de tráfego e negação de serviço.
- e) negação de serviço e falsidade.

31 - Os sistemas de detecção de intrusão (IDS) em redes de computadores podem ser classificados em

- I. Network Intrusion Detection System.
- II. Protocol-Based Intrusion Detection System.
- III. Host-Based Intrusion Detection System.

Está correto o que se afirma em

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

32 - Analise as seguintes afirmações sobre criptografia:

I - A criptografia simétrica realiza a cifragem e decifragem de informação através de algoritmos que utilizam a mesma chave.

II - A criptografia de chave pública operam com duas chaves distintas: chave privada e chave pública.

III - O resumo criptográfico é obtido através de uma função de hash (espalhamento).

IV - O SSL é uma implementação popular da criptografia de chave pública.

Está(ão) correta(s):

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

33 - Ao preencher um formulário na Internet, um usuário recebe uma mensagem de aviso informando que os dados podem ser visualizados por outra pessoa. Essa mensagem indica que a(o)

- a) página não possui criptografia.
- b) Internet está desconectada.
- c) firewall bloqueou o acesso à página.
- d) formulário está incompleto.
- e) computador está infectado por vírus.

34 A respeito de segurança da informação, assinale a opção correta.

- a) Cavalo-de-troia é um programa que se instala a partir de um arquivo aparentemente inofensivo, sem conhecimento do usuário que o recebeu, e que pode oferecer acesso de outros usuários à máquina infectada.
- b) A disponibilidade da informação é a garantia de que a informação não será alterada durante o trânsito entre o emissor e o receptor, além da garantia de que ela estará disponível para uso nesse trânsito.
- c) O uso de um programa anti-spam garante que software invasor ou usuário mal-intencionado não acesse uma máquina conectada a uma rede.
- d) A criptografia é uma das formas de garantir que a informação fique em uma área fora da rede, cujos dados somente são acessados, fisicamente, por pessoas autorizadas.
- e) Uma das formas de se garantir a segurança das informações de um website é não colocá-lo em rede, o que elimina a possibilidade de acesso por pessoas intrusas.