1 – O equipamento do tipo FIREWALL usado em redes é aquele que:

a) converte o sinal digital recebido do computador em sinal analógico e o transmite para uma linha telefônica.
b) realiza BACKUP das informações de segurança de uma rede, tais como arquivos de configuração, relação de acessos e arquivos de senha.
c) amplifica o sinal recebido por um segmento de rede e o envia para outro segmento, de forma a aumentar o comprimento total da rede.
d) analisa todo o tráfego de mensagens entrando ou saindo de uma rede, verificando quais mensagens têm autorização para isso.
e) retransmite a informação recebida por uma de suas linhas para todas as demais, sem considerar o endereço de destino dos pacotes.

2 – A fim de melhorar o desempenho no acesso à Internet, uma empresa utiliza um dispositivo que mantém a gravação das páginas acessadas por meio da técnica de armazenamento em CACHE. Qual dos processos apresentados abaixo habitualmente realiza esta tarefa?

a) BRIDGE
b) KEYSERVER
c) PROXY
d) Roteador
e) SWITCH

3 – Que tipo de mecanismo objetiva garantir a integridade da rede por meio do monitoramento de todo o tráfego de dentro para fora da rede, e vice versa, em que somente o tráfego autorizado pela política de segurança pode atravessá-lo?

a) BACK OFF
b) FIREWALL
c) FOWARD
d) HANDOFF
e) PROXY

4 – Em um ambiente WEB, qual é a finalidade do PROXY?
a) Gerenciar os erros das páginas WEB.
b) Verificar o tamanho dos pacotes recebidos do nó origem.
c) Manter o CACHE das páginas WEB mais visitadas.
d) Melhorar a capacidade de armazenamento das páginas WEB no servidor da rede.
e) Apagar as páginas mais visitadas para não sobrecarregar o CACHE.

5 – Coloque F (Falso) ou V (verdadeiro) nas afirmativas abaixo, sobre segurança de redes de computadores assinalando a seguir a opção correta.

( ) O SECURE SHELL (SSH) é um protocolo que utiliza criptografia para acesso a um computador remoto, permitindo a execução de comandos, transferência de arquivos, entre outros.

( ) O DISTRIBUTED DENIAL OF SERVICE (DDoS) é 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.
( ) BACKDOOR é um programa que permite ao invasor retornar a um computador comprometido, sendo que a existência de um BACKDOOR em uma máquina está sempre associada a uma invasão.
( ) SPYWARE é o termo utilizado para se referir a uma categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros.
( ) WORM é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador, embutindo cópias de si mesmo em outros programas ou arquivos, necessitando ser explicitamente executado para se propagar.

a) (F) (V) (V) (F) (F)
b) (F) (F) (V) (V) (F)
c) (F) (F) (V) (F) (F)
d) (V) (F) (F) (F) (V)
e) (V) (V) (F) (V) (F)

6 – Assinale a opção correta com relação às práticas de segurança em redes de computadores:

a) Uma instalação de servidor que possa ser considerada segura começa com a instalação de todos os pacotes e componentes disponíveis, especialmente os que implementam serviços de rede.
b) Para impedir que um servidor SMTP seja utilizado para envio de SPAM, ele deve ser configurado com o RELAY aberto.
c) A verificação e instalação de correções (PATCHES, FIXES, SERVICE PACKS) só são necessárias para servidores que não utilizam licença oficial.
d)Desativar os serviços não utilizados por um servidor, não aumenta a segurança, em função dos mesmos não estarem sendo utilizados.
e)Servidores PROXY mal configurados podem ser utilizados por usuários externos como “trampolim” para acessar recursos de forma anônima.

7 – Quanto a segurança de redes de computadores, é correto afirmar que:
a) na criação de uma senha segura deve-se utilizar palavras que façam parte de dicionários ou datas significativas para o criado da senha a fim de evitar o esquecimento das mesmas.
b) as senhas podem ser utilizadas com total segurança em computadores de terceiros tais como LAN HOUSES, CYBERCAFES, desde que o usuário se certifique que ninguém o observa durante a digitação da mesma.
c) é impossível a leitura de qualquer senha enquanto a mesma trafega pela rede, tendo em vista que todas as senhas trafegam criptografadas.
d) uma senha segura deve possuir letras maiúsculas, minúsculas, números e caracteres especiais para aumentar a segurança da mesma.
e)a engenharia social é um método de ataque utilizado para gerar um grande tráfego de dados em uma rede de modo que qualquer computador desta rede fique indisponível.

8 – Analise as afirmativas abaixo em relação à segurança em redes de computadores.

I – Na criptografia por chave secreta tanto o emissor quanto o receptor devem possuir a mesma chave única.
II – Na assinatura digital é utilizado o conceito de chave única por esta ser mais eficiente e segurança que a chave pública.
III – Na criptografia por chave pública são utilizadas duas chaves, uma para criptografia e outra para decriptação, sendo que a chave utilizada para criptografia pode ser pública sem comprometer o sigilo.
IV – Transações bancárias e comerciais via WEB utilizando o protocolo SECURE SOCKET LAYER (SSL) utilizam criptografia por chave única e por chave pública.
Assinale a opção correta:

a) Apenas as afirmativas I e III são verdadeiras.
b) Apenas as afirmativas I, III e IV são verdadeiras.
c) Apenas as afirmativas II e IV são verdadeiras.
d) Apenas as afirmativas II, III e IV são verdadeiras.
e) As afirmativas I, II, III e IV são verdadeiras.

9 – Assinala a opção correta com relação às vulnerabilidades de segurança:

a) A principal função da DESMILITARIZED ZONE (DMZ) é proteger a rede interna contra ataques.
b) A reutilização de senhas e utilização de senhas DEFAULT, não comprometem a segurança da informação.
c) A utilização do TELNET no acesso remoto é mais seguro que o SSH, pois o TELNET possui recurso de senha criptografada ao contrário do SSH.
d) Ao instalar um FIREWALL em uma rede, pode-se considerar que a mesma esta absolutamente segura contra invasores.
e) O FIREWALL protege uma rede tanto de ataques externos, quanto de ataques que partam de dentro da rede por ele protegida.

10 – Coloque F (Falso) ou V (Verdadeiro) nas afirmativas abaixo, em relação aos cuidados no uso da INTERNET, assinalando a seguir a opção correta.

( ) Evitar a utilização de programa leitor de EMAIL como BROWSER, desligando as opções de execução de JAVASCRIPT e Java e o modo de visualização de EMAILS no formato HTML.
( ) Arquivos anexados à mensagens enviados por pessoas ou instituições conhecidas podem ser executadas com segurança, por ser impossível fraudar o endereço do remetente de um EMAIL.
( ) Bloquear POP-UP WINDOWS e permití-las apenas para SITES conhecidos e confiáveis, onde forem realmente necessárias.
( ) LINKS no conteúdo do EMAIL podem ser acessadas com segurança, tendo um antivírus ativo e atualizado, sendo desnecessário o acesso diretamente no BROWSER.
( ) Programas ACTIVE-X, mesmo provenientes de SITES desconhecidos, podem ser executados com segurança desde que o computador disponha de um software de INTRUSION DETECTION SYSTEM (IDS)

a) (F) (V) (F) (V) (V)
b) (F) (F) (V) (F) (V)
c) (V) (V) (F) (V) (V)
d) (V) (F) (V) (F) (F)
e) (F) (V) (F) (V) (F)

11 – Analise as afirmativas abaixo em relação à segurança em redes de computadores.

I – Um sistema de detecção de intrusão (IDS – INTRUSION DETECTION SYSTEM) é um programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas.
II – INTRUSION DETECTION SYSTEM (IDS) não deve ser instalado em redes que utilizam VPN, pois a VIRTUAL PRIVATE NETWORK será sempre tratada como sendo um ataque falso positivo.
III – O termo “falso positivo” é utilizado para designar uma situação em que um FIREWALL ou INTRUSION DETECTION SYSTEM (IDS) aponta para uma atividade como sendo ataque, quando na verdade esta atividade não é um ataque.
IV – FIREWALL pessoal é um SOFTWARE ou programa utilizado para proteger um computador contra acessos não autorizados, quando configurado corretamente, substitui o uso de antivírus.
Assinale a opção correta:

a) Apenas as afirmativas I e III são verdadeiras.
b) Apenas as afirmativas I, II e III são verdadeiras.
c) Apenas as afirmativas I, II e IV são verdadeiras.
d) Apenas as afirmativas II e III são verdadeiras.
e) As afirmativas I, II, III e IV são verdadeiras.

12 – Que protocolo é utilizado para aumentar a segurança em redes de computadores sem fio?

a) TELNET
b) WPA
c) WLAN
d) PDA
e) VLAN

13 – Coloque F (Falso) ou V (Verdadeiro) nas afirmativas abaixo, em relação à prevenção contra riscos causados por vírus, assinalando a seguir a opção correta.

( ) Configurar o antivírus para verificar os arquivos obtidos pela INTERNET, HDs, disquetes e unidades removíveis, como, CD, DVD e PEN DRIVE.
( ) Utilizar, na elaboração de documentos, formatos menos suscetíveis à propagação de vírus, tais RTF, PDF ou POSTSCRIPT.
( ) Utilizar, no caso de arquivos comprimidos, o formato executável.
( ) Executar ou abrir arquivos recebidos por EMAIL, mesmo que venham de pessoas conhecidas, sem que o mesmo seja verificado pelo programa antivírus, pode ocasionar contaminação.

a) (F) (F) (V) (V) (F)
b) (V) (F) (V) (F) (F)
c) (V) (V) (F) (F) (V)
d) (F) (V) (V) (V) (F)
e) (F) (F) (F) (V) (V)

14 - Em relação à segurança em redes, assinale a opção correta.

a) SPAM é um termo usado para se referia aos e-mails solicitados, que geralmente são enviados para um grande número de pessoas, sendo seu conteúdo, exclusivamente, comercial.
b) A utilização do protocolo SSH para acesso a um computador remoto é menos seguro do que o uso de TELNET, pois o primeiro (SSH) não utiliza criptografia dos dados.
c) Um FIREWALL é um dispositivo constituído pela combinação de software e hardware, utilizado para dividir e controlar o acesso entre redes de computadores.
d) Um SPYWARE é um dispositivos ou programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários) em casos em que estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia.
e) Em SCANNER é um programa utilizado em redes de computadores, com o intuito de verificar o nível de utilização da largura de banda de rede.

15 – Em relação à Segurança de rede, assinale a opção que completa corretamente as colunas das sentenças abaixo:

I – "Um ataque de Denial of Service (DoS) contra uma rede de computadores afeta, primeiramente, o requisito _____ de segurança em redes."
II – "A Criptografia de chave _____ é utilizada nos processos de assinatura digital e não necessita de compartilhamento de chave secreta entre as entidades participantes"
III – "Nos ataques de _____, normalmente, o atacante se faz passar por outra pessoa e utiliza meios, como uma ligação telefônica ou e-mail, para persuadir o usuário a fornecer informações ou realizar determinadas ações."
IV – "_____ são e-mails que possuem como remetente ou apontam como autora da mensagem conteúdos alarmantes ou falsos e que, geralmente, têm como remetente ou apontam como autora da mensagem alguma instituição , empresa importante ou órgão governamental."

a) Integridade / Pública e Privada / Phishing / Hoax
b) Confidencialidade / única / Engenharia Social / Scam
c) Disponibilidade / Pública e Privada / Engenharia Social / Hoax
d) Integridade / Única / Phishing / Boatos
e) Disponibilidade / Assimétrica / Phishing / Scam

16 – Quanto aos aspectos de Segurança em uma WLAN (Padrão IEEE 802.11), de acordo com a Cartilha de Segurança para a Internet do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR), qual das sequências de configurações e/ou procedimentos a seguir melhor minimiza os riscos de segurança na utilização dessa tecnologia?

a) WEP, desabilitar broadcast de SSID e desabilitar filtro de MAC Address.
b) WPA, desabilitar broadcast de SSID e desabilitar modo ad-hoc.
c) 802.1x, habilitar broadcast de SSID e manter configurações default.
d) WPA, habilitar broadcast de SSID e utilizar chaves (senhas) de 128 bits.
e) WEP, habilitar filtro de MAC Address e manter configurações default.

17 – Quanto à classificação dos códigos maliciosos(Malware), qual das opções abaixo NÃO apresentam uma definição correta.

a)Vírus – é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, iste é, inserindo cópias de si mesmo e se tornando parte de outro programas e arquivos de um computador.
b) Worm – programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. O worm embute várias cópias de si mesmo em outros programas ou arquivos e necessita ser explicitamente executado para se propagar.
c) Spyware – termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Pode ser utilizado de forma legítima, mas, na maioria das vezes, é utilizado de forma dissimulada, não-autorizada e maliciosa.
d) Keylogger – programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário, como, por exemplo, após o acesso a um site de comércio eletrônico ou Internet Banking, para a captura de senhas bancárias ou números de cartões de crédito.
e)Cavalo de Tróia – programa normalmente recebido como um "presente" (exemplo: cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

18 – Em relação à segurança de redes, analise as afirmativas abaixo:

I – Cookies são pequenas informações que os sites visitados por um internauta podem armazenar em seu browser, tais como guardar a identificação e senha quando se navega de uma página para outra.
II – Permitir que programas ActiveX sejam executados em um computador apenas quando vierem de sites conhecidos e confiáveis é uma boa medida de segurança na configuração de um browser.
III – Um antivírus não é capaz de impedir que um atacante tente explorar alguma vulnerabilidade existente no Sistema Operacional de um computador, haja vista que o procedimento adequado para se evitar risco de exploração é a aplicação das correções (PATCHES) do Sistema Operacional.
IV – Uma boa senha deve ter pelo menos oito caracteres e deve mesclar letras, números e símbolos.

Assinale a opção correta.

a) Apenas a afirmativa IV é verdadeira.
b) Apenas as afirmativas II, III e IV são verdadeiras.
c) Apenas as afirmativas I e II são verdadeiras.
d) Apenas as afirmativas I, II e III são verdadeiras.
e)As afirmativas I, II, III e IV são verdadeiras.

19 – Em relação à Segurança de Redes, assinale a opção correta.

a)A implementação de UCE é cada vez mais comum em instituições, pois permite a construção de uma rede segura utilizando redes públicas (Ex. Internet) através de criptografia.
b) A implementação de SSL fornece confidencialidade e Integridade na comunicação entre um cliente e um servidor, através do uso de criptografia (Ex.: conexões HTTPS).
c) O uso do protocolo HTTP é mais seguro do que o protocolo HTTPS, pois o primeiro utiliza uma suíte criptográfica com algoritmo mais robusto.
d) Uma VPN (Video Public Network) é o protocolo mais segura para aplicações multimídias, servindo de base para um sistema de TV-Digital.
e)O protocolo HTML é amplamente utilizado para a proteção de arquivos que trafegam em aplicativos FTP (File Transfer Protocol).

20 – Um administrador de redes, ao chegar a seu local de trabalho pela manhã, constatou que o servidor WEB de sua instituição, o qual hospeda o site de e-commerce, estava "fora do ar" e que a base de dados com informações cadastrais de clientes foi copiada indevidamente. Quais requisitos básicos de Segurança em Redes foram afetados nesse incidente de segurança?

a)Integridade e Confidencialidade.
b) Disponibilidade e Integridade.
c) Integridade e Privacidade.
d) Confidencialidade e Privacidade.
e) Disponibilidade e Confidencialidade.

21 – Quanto aos aspectos de Segurança de Redes, um dos maiores problemas no gerenciamento dos alertas de um IDS (Intrusion Detection System) está no balanceamento entre "Falsos Positivos" e "Falsos Negativos". "Falso Positivo" significa ataque:

a)não detectado.
b) detectado.
c) mal classificado.
d) inexistente.
e)desconhecido.

22 – Quanto à segurança em Redes Sem Fio (Wireless), qual característica, pertencente aos padrões sem fio, é fonte (Origem) das maiores vulnerabilidades dessa tecnologia?

a)Compartilhamento do meio de transmissão e recepção.
b) Broadcast SSID.
c) Criptografia de camada 2.
d) Ausência de mecanismo de autenticação.
e)Utilização do protocolo WPA.

23 – Em redes de computadores, o padrão de interoperabilidade aprovado pelo Institute of Electrical and Electronics Engineers (IEEE) para as redes sem fio metropolitanas (WMAN) ou WIMAX é o IEEE:

a)802.3
b) 802.11
c) 802.15
d) 802.16
e)802.20

24 - Assinale a opção que completa corretamente as lacunas da sentença abaixo:
As técnicas criptográficas permitem que um remetente _____ os dados de modo que um _____não consiga obter nenhuma informação com base nos dados interceptados.

a) disfarce / conhecido
b) disfarce / intruso
c) transmita / intruso
d) apague / intruso
e) transmita / conhecido

25 – Um desconhecido liga para uma casa e diz ser do suporte técnico do provedor de acesso a Internet. Nessa ligação ele diz que a conexão com a Internet dessa casa está apresentando um problema de lentidão ao acessar a rede mundial de computadores. Então, pede a senha para corrigir o problema, além de oferecer um desconto na mensalidade do mês seguinte em virtude dos problemas ocasionados. A pessoa que recebeu a ligação inocentemente informa a senha. Após alguns dias descobre que algumas informações importantes existentes no computador foram apagadas; foi realizada uma transferência bancária; e na fatura do cartão de crédito apareceu uma compra de um computador no valor de R$ 2.352,00.
O método de ataque utilizado para persuadir o dono do computador a fornecer a sua senha é denominada Engenharia:

a) Reversa.
b) Indutiva.
c) Psicossocial.
d) Persuasiva
e) Social.

26 – Segundo a Cartilha de Segurança para Internet, um computador (ou sistema computacional) é dito seguro se este atende a três requisitos básicos relacionados aos recursos que o compõem, que são:

a) Confidencialidade, legitimidade e disponibilidade.
b) confidencialidade, integridade e acesso.
c) legitimidade, integridade e disponibilidade.
d) confidencialidade, integridade e disponibilidade.
e) confidencialidade, sigilo e disponibilidade.

27 – São programas capazes de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. São programas capazes de armazenar a posição do cursos e a tela apresentada no monitor, nos momentos em que o mouse é clicado.
As definições acima referem-se, respectivamente, a:

a) Screenlogger e Keylogger.
b) Keylogger e Screenlogger.
c) Screensaver e Keylogger.
d) Keysaver e Screenlogger.
e) Keysaver e Screensaver.

28 – Em relação à Segurança de Redes, assinale a opção que completa corretamente as lacunas das sentenças abaixo:
I – Código malicioso ou _____ é um termo genérico que abrange todos os tipos de programas especificamente desenvolvidos para executar ações maliciosas em um computador.
II – Os _____ são programas que procuram detectar e, então, anular ou remover programas maliciosos de computador.
III – Os _____ são dispositivos constituídos pela combinação de software e hardware, utilizados para dividir e controlar o acesso entre redes de computadores.

a) Malware / Antivirus / Firewall
b) Malware / AntiSpyware / Firewall
c) Malware / Antivirus / HUB
d) Malware / Antivirus / Hoaxes
e) AntiSpyware / Antivirus / Firewall

29 – Todos os algoritmos criptográficos envolvem a substituição de um dado por outro, uma cifra é um método para criptografar dados. A cifra de César funciona tomando cada letra da mensagem do texto aberto e substituindo pela k-ésima letra sucessiva do alfabeto. Por exemplo, se k=3, então a letra ‘a’ do texto aberto fica sendo ‘d’ no texto cifrado, ‘b’ no texto aberto se transforma em ‘e’ no texto cifrado, e assim por diante. Neste caso o valor de k serve de chave. Com relação à cifra de César, não se leva muito tempo para quebrar o código, pois há somente 25 valores possíveis para as chaves. Que nome recebeu um aprimoramento da cifra de César, que possuía 26!

(10^{26}) possíveis pares de letras, em vez de 25 pares possíveis:
a) cifra monoalfabética.
b) cifra alfabética.
c) cifra monossilábica.
d) cifra silábica.
e) cifra polialfabética.

30 – Qual o termo utilizado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas?
a) Malware.
b) Firewall.
c) Spam.
d) Hoaxes.
e) Phishing.

31 – O IDS (Intrusion Detection System) é um programa, ou um conjunto de programas, cuja função é:
a) prover comunicação entre o FIREWALL e o usuário.
b) detectar atividades maliciosas ou anômalas na rede.
c) bloquear endereços de rede que contenham SPAM.
d) substituir o FIREWALL.
e) dar continuidade a um contra-ataque iniciado pelo FIREWALL.

32 – Em relação aos códigos maliciosos denominados de vírus e worms, é correto afirmar que:

a) ambos necessitam ser explicitamente executados para se propagarem.
b) vírus, embute cópias de si mesmo em outros programas ou arquivos.
c) worms embutem cópias de si mesmo em outros programas ou arquivos.
d) worms são incapazes de se propagar automaticamente através de redes.
e) diferente do vírus, o worm não causa prejuízos ao sistema.

33 – Em relação aos tipos de ataques a redes, denominados “DoS” e “DDoS”, é correto afirmar que:

a) no “DoS”, apenas computadores que rodam o sistema operacional DOS, estão suscetíveis a esse tipo de ataque.
b) “DOS” e “DDOS” são idênticos em seus mecanismos de ataque.
c) no “DDoS”, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet.
d) um antivírus, se bem configurado e atualizado, é capaz de detectar e até interromper esses tipos de ataque.
e) diferente do “DDoS”, o “DoS” utiliza um conjunto de computadores para tirar de operação um ou mais serviços.

34 – Complete corretamente as lacunas do texto abaixo e, a seguir, assinale a opção correta.

Se um Capitão-Tenente quiser enviar uma mensagem assinada para um Capitão de Fragata, aquele codificará a mensagem com sua chave _____. Neste processo será gerada uma assinatura digital, que será adicionada à mensagem enviada ao Capitão de Fragata. Ao receber a mensagem, o Capitão de Fragata utilizará a chave _____ do Capitão-Tenente para decodificar a mensagem.

a) pública / privada
b) privada / privada
c) pública / pública
d) secreta / secreta
e) privada / pública

35 – Durante uma comunicação que utiliza uma conexão segura via Web, operando com o protocolo SSL (Secure Socket Layer), no tráfego de informações entre as entidades envolvidas, é empregado o método de criptografia de:

a) chave única.
b) chave pública.
c) chave privada.
d) chaves públicas e privadas.
e) chave assimétrica.

36 – Em relação aos conceitos de segurança, assinale a opção correta:

I – Worms são programas capazes de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador.
II – Spyware é o termo utilizado para se referir a uma categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros.
III – Fishing Scam se dá através do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida e que procura induzir o acesso a páginas fraudulentas, projetadas para furtar dados pessoais e financeiros de usuários.
IV – O cavalo de Tróia distingue-se de um vírus ou de um worm por não infectar outros arquivos, nem propagar cópias de si mesmo automaticamente.
V – Sempre que possível, em uma rede sem fio (wireless), deve se usar WEP (Wired Equivalente Privacy) em substituição ao WPA (Wi-Fi Protected Acess), uma vez que este padrão pode aumentar significativamente a segurança da rede.

a) Apenas as afirmativas II, III e IV são verdadeiras.
b) Apenas as afirmativas II, III e V são verdadeiras.
c) Apenas as afirmativas I, II, IV e V são verdadeiras.
d) Apenas as afirmativas II, III. IV e V são verdadeiras.
e) Apenas as afirmativas IV e V são verdadeiras.

37 – Em relação aos conceitos de segurança, assinale a afirmativa INCORRETA:

a) Cookies são pequenas informações que os sites visitados podem armazenar no computador que executa o browser.
b) Vulnerabilidade é definida como uma falha no projeto, implementação ou configuração de um software ou sistema operacional.
c) A criptografia de chave única é um método eficiente quanto ao tempo de processamento, mas tem como principal desvantagem a necessidade de utilização de um meio seguro para que a chave possa ser compartilhada.
d) A criptografia de chave privada e pública utiliza uma única chave para codificar e decodificar mensagens, tendo um desempenho superior em relação ao tempo de processamento.
e) Quando você acessa um site com conexão segura é possível checar se o site apresentado é realmente da instituição que diz ser, através de seu certificado digital.

38 – Em relação aos conceitos de segurança, assinale a afirmativa INCORRETA.

a) Um antivírus não é capaz de impedir que um atacante tente explorar alguma vulnerabilidade existente em um computador.
b) Firewall são dispositivos constituídos pela combinação de software e hardware, utilizados para dividir e controlar o acesso entre rede de computadores.
c) Os maiores riscos de utilização de programas associados ao uso de salas de bate-papo e de programas como ICQ ou IRC estão na possível utilização de técnicas de engenharia social nos diálogos.
d) Boatos (hoaxes) são e-mails que possuem conteúdos alarmantes ou falsos que, de modo geral, não são responsáveis por grandes problemas de segurança, a não ser ocupar espaço nas caixas de e-mail de usuários.
e) Backdoor é um programa que permite ao invasor retornar a um computador comprometido, sendo que a existência de um Backdoor em uma máquina está sempre associada a uma invasão.

39 – Em relação à segurança em redes de computadores, analise as afirmativas abaixo e assinale a opção correta.

a) A assinatura digital consiste na criação de vários códigos, através da utilização de uma chave pública.
b) Atualmente, para se obter um bom nível de segurança na utilização do métodos de criptografia de chave única, é aconselhável utilizar chaves de 16 bits.
c) Uma boa prática para configurar seu leitor de e-mail de forma mais segura é ligar as opções de execução de Java Script e de programas Java, e o modo de visualização de e-mail no formato HTML.
d) Ao serem executados, os programas ActiveX podem enviar um arquivo qualquer pela Internet ou mesmo Instalar programas em seu computador.
e) O Distributed Denial of Service (DDoS) constitui um serviço de antivírus muito utilizado pelas grandes empresas.

40 – Em relação à elaboração de senhas, assinale a afirmativa INCORRETA.

a) Uma boa senha deve ter pelo menos seis caracteres.
b) Uma das regras para elaboração de senhas é jamais utilizar palavras que façam parte de dicionários.
c) Nomes, sobrenomes, números de documentos são boas senhas por serem consideradas seguras e de fácil memorização.
d) Quanto maior a senha mais difícil será descobrí-la.
e) A senha "1qaz2wsx" parece ser suficientemente "bagunçada", mas não é considerada uma boa senha, pois está associada à proximidade entre esses caracteres no teclado.

41 – Como se denomina o programa malicioso que pode capturar e armazenar as teclas digitadas pelo usuário?
a) KEYLOGGER
b) Vírus
c) PHISHING
d) Cavalo de Tróia
e) WORM

42 – Que programa malicioso tem como características não infectar outros arquivos, nem propagar cópias de si mesmo automaticamente e necessita ser explicitamente executado?

a) Vírus.
b) WORM.
c) PHISHING.
d) Cavalo de Tróia.
e) SPAM.

43 – A segurança em redes de computadores utiliza criptografia para garantir uma comunicação segura. Qual requisito básico de segurança NÃO é garantido pela criptografia?
a) Confidencialidade dos dados.
b) Integridade dos dados.
c) Não repúdio.
d) Disponibilidade dos dados.
e) Autenticidade dos dados.

44 – Um ataque de negação de serviço viola qual requisito de segurança?

a) Integridade.
b) Disponibilidade.
c) Autenticidade.
d) Confidencialidade.
e) Autorização.

45 – Um sistema cuja função é detectar atividades maliciosas ou anômalas é chamado de:

a) FIREWALL.
b) IDS.
c) PROXY.
d) Antispam.
e) Concentrador de log.

46 – Qual a diferença entre um vírus e um WORM?

a) O vírus se propaga automaticamente através de redes, enviando cópias de si mesmo de computador para computador.
b) O vírus ser propaga explorando vulnerabilidades existentes nos softwares instalados em computadores.
c) O WORM se propaga inserindo cópias de si mesmo e se tornando parte de outros programas.
d) O WORM depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo.
e) O WORM não embute cópias de si mesmo em outros programas.

47 – Como é denominado o ataque onde alguém faz uso de persuasão, abusando da ingenuidade ou confiança do usuário, no intuito de obter informações para ter acesso não autorizado?

a) Engenharia Social.
b) Negação de Serviço.
c) ARP POISON.
d)DNS POISON.
e) MAN-IN-THE-MIDDLE.

48 – Que protocolo fornece criptografia dos dados e autenticação entre um cliente e um servidor WEB?

a) WEP
b) SSL
c) ARP
d) TCP
e) FTP

49 – Que algoritmo de criptografia abaixo usa chave pública na criptografia de dados?

a) DES
b) AES
c) RSA
d) MD5
e) 3DES

50 – De acordo com os padrões existentes de equipamentos de segurança de redes de computadores, correlacione as soluções às suas respectivas características, e assinale a opção correta.

SOLUÇÕES	CARACTERÍSTICAS
I – VPN (Virtual Private Network) II – Firewall III – Firewall pessoal IV – IDS (Intrusion Detection System) V – SSL (Secure Sockets Layer) VI – Antivírus VII - Antimalware	( ) Protocolo que, por meio de criptografia, fornece confidencialidade e integridade nas comunicações entre um cliente e um servidor, podendo também ser usado para prover autenticação.
	( ) Rede que utiliza criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.
	( ) Programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas.
	( ) Dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores.

a) (V) (I) (VI) (III)
b) (I) (II) (VII) (III)
c) (V) (I) (IV) (II)
d) (I) (V) (IV) (II)
e) (V) (II) (VI) (III)

51 – Assinale a opção que NÃO apresenta um dos protocolos de segurança adotados em ambientes de redes sem fio.

a) WEP (Wired Equivalent Protocolo)
b) TKIP (Temporal Key Integrity Protocolo)
c) AES (Advanced Encryption Standard)
d) WPA (Wireless Protect Access)
e) IEEE 802.15

52 – Assinale a opção que apresenta a sequência que completa corretamente as lacunas da sentença abaixo. Em segurança de redes de computadores, a _____ protege a informação contra alteração não autorizada. A _____ garante que um recurso esteja disponível sempre que necessário. E a _____ protege uma informação contra acesso não autorizado.

a) disponibilidade / integridade / confidencialidade
b) disponibilidade / confidencialidade / integridade
c) integridade / disponibilidade / confidencialidade
d) confidencialidade / integridade / confidencialidade
e) confidencialidade / disponibilidade / integridade

53 – Com relação às características dos códigos maliciosos atualmente existentes no âmbito da segurança da informação, é correto afirmar que programa vírus é um programa.
a)projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.
b) ou parte de um programa de computador, que se propaga inserindo cópias de si mesmo, tornando-se parte de outros programas e arquivos. Depende da execução do programa ou arquivos hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.
c) capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar.
d) normalmente recebido como um presente (por exemplo, cartão virtual álbum de fotos, protetor de tela, jogo etc.) que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, sem o conhecimento do usuário.
e) capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Normalmente sua ativação é condicionada a uma ação prévia do usuário, como o acesso a um site especifico de comércio eletrônico.

54 – Qual protocolo assegura que os dados transmitidos entre cliente e servidor utilizem recursos de autenticação e criptografia?

a) HTTP
b) DNS
c) SNMP
d) SMTP
e) SSH

55 – O conjunto de caracteres utilizados no processo de identificação do usuário, assegurando que o usuário é realmente determinado indivíduo, e que possui o direito de acessar o recurso computacional em questão, é denominado:

a) malware
b) cookie
c) senha
d) worm
e) token

56 – Assinle a opção que descreve corretamente a técnica denominada SPAM, utilizada pelos ataques cibernéticos.

a) Tipo de golpe por meio do qual um golpista tenta obter dados pessoais e financeiros de um usuário pela utilização combinada de meios técnicos e engenharia social.
b) Termo usado para se referir aos e-mails não solicitados que, geralmente, são enviados para um grande número de pessoas.
c) Mensagem que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente, ou aponta como autor, alguma instituição, empresa importante, ou órgão governamental.
d) Esquemas ou ações enganosas e/ou fraudulentas. Normalmente, têm como finalidade obter vantagens financeiras.
e) Envolve o redirecionamento da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS.

57 – Considere que K^{+A} e K^{-A} são as chaves públicas e privadas do usuário A, respectivamente, que K^{+B} e K^{-B} são as chaves públicas e privadas do usuário B, e que "m" é uma mensagem em texto que A deseja enviar para B com confidencialidade. Com base nesses dados, assinale a opção correta.

a) O usuário A deve informar K^{-A} ao usuário B antes de transmitir m.
b) O usuário B deve disponibilizar K^{-B} ao usuário A antes de transmitir m.
c) $K^{+A}(m) = K^{-B}(m)$. A mensagem criptografada pelo usuário A, com a sua chave pública, é igual à mensagem criptografada com chave privada do usuário B.
d) $K^{+B}(m) = K^{-B}(m)$. A mensagem
e) $K^{-B}(K^{+B}(m)) = m$. O usuário A deve cifrar a mensagem m com a chave pública do usuário B. Por outro lado, o usuário B deve aplicar sua chave privada para recuperar o texto cifrado.

58 – Assinale a opção que corresponde a um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário.

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

59 – Qual recurso é utilizados para proteger um computador contra acessos não autorizados vindos da Internet?

a) Firewall.
b) Webmail.
c) Spam.
d) Antivírus.
e) Backup.

60 – Assinaturas digitais são utilizadas para que:

a) o receptor possa verificar a identidade alegada pelo transmissor.
b) o receptor tenha a possibilidade de forjar, ele mesmo, a mensagem.
c) o transmissor possa repudiar, posteriormente, o conteúdo da mensagem.
d) o receptor não possa verificar a identidade alegada
e) o receptor possa cifrar mensagens usando a chave privada do transmissor.

61 – Segundo a Cartilha de Segurança para Internet (2012), o que deve ser usado na elaboração de senhas?

a) Qualquer tipo de dado pessoal.
b) Palavras que façam parte de listas.
c) Sequências de teclado.
d) Diferentes tipos de caracteres.
e) Salvar as senhas no navegador Web.

62 – Assinale a opção que corresponde a um método criptográfico que usa chaves assimétricas.

a) RSA
b) AES
c) Blowfish
d) RC4
e) 3DES

63 – Qual é a técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet?

a) Varredura em redes.
b) Falsificação de e-mail.
c) Força Bruta.
d) Desfiguração de página.
e) Negação de serviço distribuído.

64 – Assinale a opção correta com relação à definição de VULNERABILIDADE.

a) Consiste em efetuar buscas minunciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles, como, por exemplo, serviços disponibilizados e programas instalados.
b) Consiste em alterar campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.
c) Condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Alguns exemplos dessa condição são as falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede.
d) Consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos.
e) Consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços com o nome e os mesmos privilégios desse usuário.

65 – Como se denominam os programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador?
a) Códigos maliciosos (malwares)
b) SPAM
c) Firewall.
d) Cookies.
e) Antivírus.

66 – Qual é o mecanismo de segurança que define os direitos e as responsabilidades de cada um em relação à segurança dos recursos computacionais que utiliza e às penalidades às quais o indivíduo está sujeito, sendo considerado importante tanto para as instituições como para os usuários, pelo fato de deixar claro o comportamento de cada um?

a) Notificação de incidentes e abusos.
b) Políticas de segurança.
c) Contas e senhas.
d) Criptografia.
e) Registro de eventos (Logs)

67 – Correlacione os requisitos básicos de segurança às suas respectivas definições e assinale a opção que apresenta a sequência correta.

I – Identificação
II – Autenticação
III – Autorização
IV – Integridade
V – Confidencialidade
VI – Não repúdio
VIII – Disponibilidade

( ) Evitar que uma entidade possa negar que foi ela quem executou uma ação.
( ) Determinar as ações que a entidade pode executar.
( ) Verificar se a entidade é realmente quem ela diz ser.
( ) Garantir que um recurso esteja disponível sempre que necessário.
( ) Proteger a informação contra alteração não autorizada.

( ) Proteger a informação contra acesso não autorizado.
( ) Permitir que uma entidade se identifique, ou seja, diga quem ela é.
( ) Filtrar o tráfego de dados de Entrada/Saída de uma rede local.

a) (VI) (III) (II) (VII) (IV) (V) (I) (-)
b) (III) (-) (II) (I) (V) (IV) (VIII) (VI)
c) (VI) (VII) (II) (I) (-) (IV) (III) (V)
d) (III) (V) (I) (IV) (II) (VI) (VII) (-)
e) (I) (-) (III) (VI) (V) (II) (IV) (VII)

68 – Qual é o mecanismo de segurança que é considerado como a ciência e a arte de escrever mensagens em forma cifrada ou em código?

a) Firewall.
b) IDS.
c) Criptografia.
d) Antivírus.
e) Anti-Spam.

69 – Assinale a opção correta com relação à definição de “VÍRUS”.

a) Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador, porém não se propaga por meio dessa inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.
b) Programa usado para proteger um computador contra acesso não autorizados vindos da Internet.
c) Rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots.
d) Dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores.
e) É um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Para que possa se tornar ativo e dar continuidade ao processo de infecção, depende da execução do programa.

70 – Coloque F (falso) ou V (verdadeiro) com relação aos elementos que devem ser usados na elaboração de boas senhas, assinalando, a seguir, a opção que apresenta a sequência correta.
( ) Números aleatórios.
( ) Diferentes tipos de caracteres.
( ) Sequência de teclado.
( ) Palavras que façam parte de listas.
( ) Grande quantidade de caracteres.

a) (V) (F) (V) (F) (F)
b) (F) (F) (V) (V) (V)
c) (V) (V) (F) (F) (V)
d) (V) (V) (V) (V) (F)
e) (V) (F) (F) (V) (V)

71 – Qual é o mecanismo da criptografia que permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isso e que ela não foi alterada?

a) Assinatura Digital.
b) Codificação.
c) Decodificação.
d) Chave.
e) Função de Resumo (Hash)

72 – Qual é o tipo de fraude que ocorre por meio de envio de mensagens eletrônicas (“iscas”) que tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio de acesso a páginas falsas, que tentam se passar pela página oficial da instituição, da instalação de códigos maliciosos, projetados para coletar informações sensíveis, e do preenchimento de formulários contidos na mensagem ou em páginas Web?

a) PHARMING
b) Boato (HOAX)
c) Varredura em redes (SCAN)
d) Falsificação de e-mail (SPOOFING)
e) PHISHING