1) Sobre a especificação 10baseT é correto afirmar que:
a) O meio de transmissão é o cabo coaxial fino de 300 Ohms;
b) A maior taxa de transmissão suportada é de 100Mbps a distâncias de até 200 Metros.
c) No caso de a rede possuir mais de dois dispositivos conectados, o uso de HUBS (repetidores) se torna obrigatório.
d) O conector é o BNC

2) Sobre as categorias de cabo par-trançado:

a) As categorias 1 e 2 são utilizadas somente em ligações telefônicas. A categoria 3 transmite no máximo 26 Mbps. Categoria 4 transmite no máximo 100Mbps. A categoria 5 transmite no máximo 10Gbps.
b) As categorias 1 e 2 são utilizadas somente em ligações telefônicas. A categoria 3 transmite no máximo 16 Mbps. A categoria 4 transmite no máximo 20 Mbps. A categoria 5 transmite no máximo 1Gbps.
c) As categorias 1 e 2 são utilizadas nas redes de computadores. A categoria 3 transmite no máximo 16 Mbps. A categoria 4 transmite no máximo 200 Mbps. A categoria 5 transmite no máximo 10Gbps.
d) As categorias 1 e 2 são utilizadas nas redes de computadores. A categoria 3 transmite no máximo 10 Mbps. A categoria 4 transmite no máximo 20 Mbps. A categoria 5 transmite no máximo 1Gbps.

3) A respeito do processo de flooding é correto afirmar:
a) Os hubs fazem flooding em todas as transmissões;
b) O Switch faz flooding independentemente da quantidade de tempo em que esteja ligado;
c) Os roteadores fazem flooding somente nos primeiros minutos depois de serem ligados;
d) O processo de flooding não é mais implementado em nenhum equipamento ativo de rede.

4) Temos duas estações A e B em rede. A estação A envia um pacote em Broadcast que deveria ser recebido pela estação B. Em quais situações a seguir o pacote será efetivamente recebido?
a) A e B estando no mesmo seguimento coaxial.
b) A e B estão em HUBS diferentes, ligados em cascata.
c) A e B estão em HUBS diferentes, cada um ligado em uma placa de rede diferente do servidor.
d) A e B estão em HUBS diferentes, cada um ligado a uma porta de um mesmo SWITCH.
e) A e B estão em portas diferentes do SWITCH padrão
f) A e B estão em portas diferentes de um SWITCH camada 3, cada qual configurado para uma VLAN diferente.
g) A está conectada remotamente (via RAS do NT ou Netware Conect, por exemplo) à rede empresa, onde se encontra B.

a) (a) sim (b) sim (c) não (d) sim (e) sim (f) não (g) não
b) (a) não (b) sim (c) sim (d) sim (e) sim (f) não (g) não
c) (a) sim (b) não (c) não (d) sim (e) sim (f) não (g) sim
d) (a) sim (b) sim (c) não (d) não (e) não (f) não (g) não

5) O TCP/IP possui um esquema de endereçamento em que é possível definir o endereço da rede e o endereço do HOST. É dividido normalmente em três classes básicas (A,Be C), além de uma para multicast (D) e outra para endereçamento especial. A respeito dos endereços do IP classes A, B e C, julgue os seguintes itens:

a) Um endereço classe A é caraterizado por ter o primeiro bit definido como zero.
b) Um endereço classe B é caracterizado por ter seu primeiro bit definido como 1 e o segundo bit definido como 1.
c) Um endereço classe C é caracterizado por ter seu primeiro bit definido com 1 o segundo bit definido como 0 e o terceiro bit definido como 1.
d) Um endereço classe C é caracterizado por ter seu primeiro bit definido como 0, o segundo bit como 1 e o terceiro como 1.

6) Um Switch Ethernet desempenha a seguinte função na rede:
a) Distribui endereços IP para todos os hosts da rede;
b) Realiza comutação de quadros na camada 2 do modelo OSI.
c) Realiza endereçamento de pacotes, processamento o endereço IP destino em função de uma tabela de rotas.
d) Gerencia conexões VOIP, fazendo a tradução de padrões quando necessário.
e) Repete todos os quadros recebidos em todas as suas interfaces.

7) Sobre implementação de firewalls, considere as seguintes afirmativas:
I - O sistema de conversão de endereços de rede pode modificar os números de porta de origem e destino dos pacotes.
II – Em um firewall baseado em regras, é possível identificar o primeiro pacote de uma conexão UDP pelo bit SYN ativo no cabeçalho.
III – O rastreamento de conexões (connection tracking) é necessário apenas para manter um registro de atividade (log) das conexões. Um firewall baseado em regras poderia funcionar perfeitamente sem rastreamento de conexões. IV – Para liberar o tráfego para um servidor DNS na rede interna, basta abrir a porta UDP 63.
V – Uma vantagem de utilizar um proxy de aplicação é poder filtrar as requisições do usuário.
Assinale a alternativa correta:
a) Somente as afirmativas I, II e IV são verdadeiras.
b) Somente as afirmativas II, III e V são verdadeiras.
c) Somente as afirmativas I, IV e V são verdadeiras.
d) Somente as afirmativas I e V são verdadeiras.
e) Somente a afirmativa II é verdadeira

ANULADA

8) Considere as seguintes afirmativas sobre o Firewall:
I – A função do Firewall é somente impedir que a rede interna seja alvo de ataques internos;
II – Uma política de segurança possível afirma que tudo que não está explicitamente permitido, é proibido.
III – Um Firewall deve permitir que seja realizada a conversão do endereço via NAT (Network address Tranaslation) e a realização de IP Spoofing. IV – Um Firewall pode ser utilizado para evitar o sniffing dentro da rede interna.
V – Para aplicações como FTP, pode ser necessário que o firewall analise o protocolo no nível de aplicação.
Assinale a alternativa correta:
a) Somente as afirmativas II e V são verdadeiras;
b) Somente as afirmativas III e V são verdadeiras;
c) Somente as afirmativas I e II são verdadeiras;
d) Somente as afirmativas I,II e III são verdadeiras;
e) Somente as afirmativas II e IV são verdadeiras;

9) Uma empresa precisa ligar um edifício coligado que se encontra a aproximadamente 250m de distância da sede principal. Qual das seguintes tecnologia Ethernet permitirá essa ligação sem a necessidade de repetidores? Escolha a melhor.
a) Cabo padrão 10base2
b) Cabo padrão 10baseT
c) Cabo padrão 10baseFL
d) Cabo padrão 10base5

10) Qual dos seguintes conjuntos de parâmetros TCP/IP são o mínimo necessário para que um computador possa se comunicar com a Internet?
a) Endereço Ip, gateway padrão;
b) Endereço Ip, máscara de sub-rede.
c) Endereço IP, máscara de sub-rede, gateway padrão.
d) Endereço IP, gateway padrão, Servidor DNS primário.

11) Quais critérios devem ser avaliados para a escolha de uma classe de endereçamento IP?
a) A região de localização
b) O número de endereços IP necessários
c) Depende da marca dos equipamentos
d) Nenhuma das alternativas acima

12) Qual das seguintes opções descreve a máscara de sub-rede?
a) Essa camada seta os bits que correspondem à rede para um e seta os bits que correspondem aos equipamentos para zero.
b) É uma sequência de 16 bits.
c) É utilizada para endereçar os computadores na rede.
d) Os roteadores não utilizam esse endereço.

13) Sobre os Ips reservados é correto afirmar:
a) O endereço 0.0.0.0 é reservado para broadcast na rede local.
b) O endereço 1.0.0.127 é conhecido como Loopback.
c)O endereço 169.254.1.1 está na faixa de endereços classe C.
d) O endereço 255.255.255.255 é reservado com endereço de broadcast.

14) Em relação ao protocolo ARP, quando a estação remetente deseja resolver (descobrir) o endereço físico (exemplo Ethernet) da estação de destino a partir do endereço Ip desta última, ele envia uma mensagem de solicitação.
a) Para o endereço de broadcast limitado 255.255.255.255. A estação de destino responde ao pedido diretamente para a estação solicitante.
b) Diretamente para o servidor ARP, enquanto o servidor ARP responde ao pedido diretamente para a estação solicitante.
c) Para o endereço de broadcast limitado 255.255.255.255 . O servidor ARP responde ao pedido diretamente para estação solicitante.
d) Diretamente para o servidor ARP. O servidor ARP responde ao pedido para o endereço de broadcast limitado 255.255.255.255.
e) Para o endereço de broadcast limitado 255.255.255.255. A estação destino responde ao pedido também para o endereço de broadcast limitado 255.255.255.255.

15) Uma máscara de rede 255.255.255.248 foi aplicada sobre o endereço 200.1.1.0/24. Essa operação irá criar:

a) 228 novos endereços de rede.
b) 3 novos endereços de rede.
c) Em cada nova rede criada, 254 novos endereços para hosts.
d) Em cada nova rede criada, 14 endereços para hosts.
e) Em cada nova rede criada, 6 endereços para hosts.

16) Uma intranet tradicional é :

a) Uma rede padrão LAN, que utiliza o protocolo TCP/IP para comunicação;
b) Uma rede coorporativa que utiliza o protocolo IPX da internet para seu transporte fundamental;
c) Composta por inumeras redes de empresas distintas;
d) Uma rede privada que permite fácil acesso a Internet, utilizando o protocolo TCP/IP, diferente de uma extranet;

17) Assinale a alternativa que descreve corretamente o comportamento do protocolo Ethernet na ocorrência de uma colisão:

a) O protocolo retransmite imediatamente;
b) O protocolo aguarda um tempo aleatório e retransmite;
c) O protocolo aguarda um tempo aleatório, verifica se há portadora no meio e, caso não haja, retransmite;
d) O protocolo aguarda o meio ficar livre e retransmite;

18) Uma colisão pode ocorrer em alguns protocolos quando duas máquinas compartilham o mesmo meio de transmissão e tentam utiliza-lo ao mesmo tempo. Considere as afirmativas a seguir relativas as colisões em redes locais.

I – Colisões podem ocorrer em redes Fast Ethernet não comutadas, ou seja, utilizando HUB.
II – Uma colisão poderá ocorrer em redes em topologias em anel, como a rede token ring;
III – Colisões Nunca ocorrem em redes ethernet comutadas, ou seja, utilizando switch.
IV– O número de colisões está diretamente relacionando ao desempenho da rede.

a) Somente as afirmativas I, III e IV são verdadeiras;
b) Somente as afirmativas I e IV são verdadeiras;
c) Somente as afirmativas II e III são verdadeiras;
d) Somente as afirmativas II, III e IV são verdadeiras;

19) Que camada do modelo OSI é responsável pelas funções de criptografia, conversão de códigos e formatação?

a) Apresentação
b) Sessão
c) Transporte
d) Física

20) O modelo de referência OSI é:
a) Padrão direcionado para interconexão homogênea.
b) Padrão de arquitetura proprietária.
c) Exemplo de sistema fechado.
d) Exemplo de sistema aberto.

21) 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.

22) 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.

23) 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.

24) Assinale a opção que corresponde a um método criptográfico que usa chaves assimétricas.

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

25) 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. DOS

27) Assinale a opção correta com relação à definição de VULNERABILIDADE.
a) Consiste em efetuar buscas minuneiosas 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 email, 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. Allguns exemplos dessas 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 adivinhas, 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.

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

30) Qual é o mecanismo de segurança que define os diretórios 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 esperado de cada um?

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

31) 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
VII – Disponibilidade

( ) Evitar que uma entidade possa negar que foi ela quem executou uma ação.
( ) Determinar as ações que na 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 uma informação contra acesso não autorizado.
( ) 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) (VII) (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)

32) Qual é o mecanismo de segurança que é considerado como a ciência e arte de escrever mensagens em forma cifrada ou em código.

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

33 - 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.

34 - Em relação aos sistemas de proteção de rede,

a) um exemplo típico de tentativa suspeita que é detectada pelo HIDS é o login sem sucesso em aplicações que utilizam autenticação de rede. Nesse caso, HIDS informará ao administrador de rede que existe um usuário tentando utilizar uma aplicação que ele não tem permissão.
b) o IPS é uma ferramenta utilizada para monitorar o tráfego da rede, detectar e alertar sobre ataques e tentativas de acessos indevidos e, embora não bloqueie uma ação, tem a capacidade de verificar se esta ação é ou não uma ameaça para um segmento de rede.
c) a função dos stateful inspection firewalls é analisar o tráfego ao nível do IP e TCP/UDP, construindo tabelas de estado das ligações à Internet para prevenir os ataques do tipo spoofing, replaying, entre outros.
d) os Proxies atuam de acordo com informação de estado, sem considerar as regras de acesso estáticas, e possibilitam o uso de filtragem com base na informação de nível de pacote.
e) os appliances NAC compõem uma arquitetura mais elaborada, pois integram soluções de terceiros na infraestrutura de rede envolvendo switches next generation com suporte à tecnologia NAC.

35 - Atualmente tem sido observado o aumento de tentativas e violações que comprometem a segurança das redes e da Internet. 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

36 - Considerados pragas digitais, os rootkits são malwares que, ao se instalarem no computador alvo:
a) apagam as principais informações do firmware da máquina infectada.
b) camuflam a sua existência e fornecem acesso privilegiado ao computador infectado.
c) desinstalam ou corrompem os aplicativos office configurados no computador infectado
d) modificam as configurações de TCP/IP do computador infectado, impedindo o acesso à Internet.
e) multiplicam-se indefinidamente até ocupar todo o espaço disponível no disco rígido.

37 - Analise as seguintes afirmativas referentes aos vírus de computador e classifique-as com V para as verdadeiras e F para as falsas.

( ) A propagação ocorre pela inserção de cópias de si mesmo e tornando-se parte de outros programas e arquivos.
( ) Entre os tipos mais comuns, podemos destacar os vírus propagados por email, de script e de macro.
( ) Para se tornar ativo e dar continuidade ao processo de infecção, depende da execução do programa ou arquivo hospedeiro.

Assinale a alternativa que apresenta a sequência CORRETA:

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

38 - No bloco superior, estão descritas características de quatro tipos de códigos maliciosos; no inferior, estão listados os nomes de três códigos. Associe adequadamente o bloco inferior ao superior.

1. Programa ou parte de um programa de computador que se propaga inserindo cópias de si mesmo, e tornando-se parte de outros programas e arquivos.
2. Programa capaz de se propagar automaticamente pelas redes, enviando cópias de um computador para outro computador.
3. Programa que possui mecanismos de comunicação com o invasor e pode ser controlado remotamente.
4. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

( ) Bot
( ) Virus
( ) Worm

A sequência correta de preenchimento dos parênteses, de cima para baixo, é

a) 3, 1 e 2.
b) 4, 1 e 2.
c) 2, 1 e 3.
d) 2, 3 e 4.
e) 1, 2 e 3.

39 - Analise as seguintes afirmativas sobre ameaças à Segurança da Informação:

I. Cavalo de Troia é um programa que contém código malicioso e se passa por um programa desejado pelo usuário, com o objetivo de obter dados não autorizados do usuário.

II. Worms, ao contrário de outros tipos de vírus, não precisam de um arquivo host para se propagar de um computador para outro.

III. Spoofing é um tipo de ataque que consiste em mascarar pacotes IP, utilizando endereços de remetentes falsos.

Estão CORRETAS as afirmativas:

a) I e II, apenas.
b) I e III, apenas.
c) II e III, apenas.
d) I, II e III.
e) Todas as alternativas estão erradas.

40 - Analise as afirmativas abaixo com relação às técnicas de invasão e assinale com (V) as verdadeiras e (F) as falsas.

( ) Phishing é o tipo de fraude em que um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e de engenharia social.

( ) Rootkit é um conjunto de programas e de técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

( ) Cavalo de Tróia é 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.

( ) Spoofing é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio de programas específicos.

( ) Scan é uma forma de efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados.

A sequência correta é

a) F, F, V, F, V.
b) F, V, F, F, F.
c) V, F, V, F, F.
d) V, F, F, V, V.
e) V, V, V, F, V.

41 - Sobre criptografia, considere:

I. A criptografia simétrica é um tipo de criptografia que usa um par de chaves criptográficas distintas (privada e pública) e matematicamente relacionadas.

II. A criptografia assimétrica é um tipo de criptografia que usa uma chave única para cifrar e decifrar dados.

III. A chave pública está disponível para todos que queiram cifrar informações para o dono da chave privada ou para verificação de uma assinatura digital criada com a chave privada correspondente; a chave privada é mantida em segredo pelo seu dono e pode decifrar informações ou gerar assinaturas digitais.

Está correto o que se afirma em:
a) I e II, apenas.
b) I e III, apenas.
c) II e III, apenas.
d) I, II e III.
e) III, apenas.