Concurso Público para o provimento de vagas em Cargos de Nível Superior da Carreira de Desenvolvimento Tecnológico

CÓDIGO DA VAGA: TP08

QUESTÕES DE MÚLTIPLAS ESCOLHAS

1) Em relação à manutenção corretiva pode-se afirmar que :

a) Constitui a forma mais barata de manutenção do ponto de vista total do sistema.
b) Aumenta a vida útil dos equipamentos e instalações.
c) Esta manutenção ocorre em momentos aleatórios podendo gerar inconvenientes ou paradas em períodos de alta demanda.
d) É importante para prevenção de falhas que possam originar paragem no sistema.
e) É realizada com base em estudos estatísticos dos equipamentos e instalações.

2) A manutenção preditiva é considerada o primeiro grande quebra de paradigma na manutenção de instalações operacionais. Com relação a este tipo de manutenção é incorreto afirmar que:

a) Esta manutenção permite a operação contínua dos sistemas e equipamentos durante o maior intervalo de tempo possível.
b) É baseada na modificação sistemática de parâmetros de desempenho ou condição.
c) Não é necessário que o sistema ou a instalação permitam qualquer tipo de monitoramento ou medição de parâmetros.
d) A decisão de intervenção é tomada quando o grau de degradação do sistema atinge um limite estabelecido.
e) Deve-se estabelecer uma relação custo-benefício para avaliar se o sistema requer este tipo de ação.

3) Ataques de negação de serviço, conhecidos como DoS (Denial of Service) constituem tentativas de tornar os recursos de um sistema indisponíneis para seus utilizadores através de invalidação por sobrecarga. Para um servidor WWW aberto não constitue uma estratégia de proteção a ataques DoS.

a) Utilização de sistemas de detecção de intrusão (IDS).
b) Utilização de conexão backup de internet com conjuntos separados de endereços de IP para usuários críticos.
c) Monitoramento do sistema e seus componentes.
d) Implementação de taxa máxima de respostas a requisições tipo SYN.
e) Utilização de autenticação segura para criação de conexões entre clientes e servidores.

Concurso Público para o provimento de vagas em Cargos de Nível Superior da Carreira de Desenvolvimento Tecnológico

CÓDIGO DA VAGA: TP08

4) A segurança da informação é usualmente definida como a prática de defesa da informação do acesso não autorizado, divulgação, interrupção, modificação, leitura, inspeção, gravação ou destruição. Esta definição é geral e pode ser utilizada independentemente dos tipos de dado fornecidos. Classicamente, os conceitos chave da segurança da informação são:

a) Livre acesso, integridade e disponibilidade
b) Livre acesso, utilidade, disponibilidade
c) Confidenciabilidade, integridade e disponibilidade
d) Controle, utilidade, segurança
e) Privacidade, controle, segurança.

5) Ameaças à segurança computacional estão relacionadas diretamente com a perda de uma de suas três características principais, a saber:

a) Acessibilidade, confidencialidade e portabilidade
b) Confidencialidade, integridade e disponibilidddade
c) Disponibilidade, portabilidade e funcionalidade
d) Integridade, acessibilidade e privacidade
e) Privacidade, responsabilidade e disponibilidade

6) Correlacione o tipo de malware da coluna à esquerda da tabela abaixo com a descrição da coluna à direita da tabela.

Malware	Descrição
I. Bactéria	a. Programa que assume outro computador na Internet e então usa-o para lançar ataques que são difíceis de para o seu criador.
II. Bomba Lógica	b. Programa que pode se replicar e enviar suas cópias de computador a computador através das conexões de rede. Em cada computador que ele chega, ele se replica e se propaga novamente. Além de propagação, ele usualmente realiza alguma função indesejada.
III. Cavalo de Tróia	c. Lógica embutida em um programa de computador que verifica se certo conjunto de condições está presente no sistema. Quando ele detecta essas condições, ele executa alguma função resultando em ações não autorizadas.
IV. Vírus	d. Programa que consome recursos do sistema por se replicar continuamente.
V. Verme (Worm)	e. Código embutido dentro de um programa que faz com que uma cópia dele próprio seja inserido em um ou mais programas. Além de propagação, ele usualmente realiza alguma função indesejada.
VI. Zumbi	f. Programa que parece ter uma função útil, mas que também tem uma função escondida e maliciosa que ilude os mecanismos de segurança, algumas vezes ao explorar autorizações legítimas de uma entidade do sistema que invoca o programa.

Assinale a alternative que represente a correlação correta:

Concurso Público para o provimento de vagas em Cargos de Nível Superior da Carreira de Desenvolvimento Tecnológico

CÓDIGO DA VAGA: TP08

a) I-a, II-b, III-c, IV-d, V-e, VI-f
b) I-d, II-c, III-f, IV-b, V-e, VI-a
c) I-d, II-f, III-c, IV-e, V-a, VI-b
d) I-d, II-c, III-f, IV-e, V-b, VI-a
e) I-a, II-c, III-e, IV-f, V-b, VI-d

7) Verifique se cada afirmação abaixo é verdadeira (V) ou falsa (F); em seguida, assinale a alternativa que apresenta a sequência correta:

( ) Ataques DoS impedem os usuários legítimos de utilizarem determinados serviços de um computador ou rede de computadores.

( ) NAS é um tipo de rede local de armazenamento projetada para lidar com grandes volumes de transferência de dados em redes de empresas que utilizam servidores high-end, várias matrizes de disco e tecnologia de interconexão Fibre Channel.

( ) A série de padrões IEEE 802 contém padrões para uso em redes de comunicação locais e metropolitanas, especialmente relacionados com as camadas 1 (physical) e 2 (data link) do modelo OSI e correspondente link layer do modelo TCP/IP. IEEE 802 refers to a family of IEEE standards dealing with local area networks and metropolitan area networks.

( ) O endereço de broadcast 127.0.0.0 é um exemplo de endereço IP reservado para a comunicação segura entre duas máquinas específicas na rede.

( ) A política de segurança é um conjunto de diretrizes, normas, procedimentos e instruções de trabalho que estabelecem os critérios de segurança para serem adotados no nível local ou a institucional, visando o estabelecimento, a padronização e a normalização da segurança tanto no âmbito humano quanto tecnológico.

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

8) Nesta questão, você tem que fornecer três palavras que foram sistematicamente removidas do texto; lacunas de texto são representadas pelos algarismos romanos maiúsculos entre parenteses: (I), (II) e (III); note que as lacunas (I) e (II) já aparecem na última linha de texto da figura abaixo.

Concurso Público para o provimento de vagas em Cargos de Nível Superior da Carreira de Desenvolvimento Tecnológico

CÓDIGO DA VAGA: TP08

Imagine um esquema de assinatura digital que use certificados X.509, como no exemplo da figura abaixo:

Certifico que a chave pública
19836A8B03030CF83737E3837837FC3s7092827262643FFA82710382828282A
pertence a
João Roberto da Silva
Avenida Brasil, 12345
Rio das Ostras, RJ 28890-000
Nascimento: 7 de setembro de 1958
E-mail: bob@supernet.com.br

(I) SHA-1 do certificado acima assinado com a chave privada da (II)

Imagine que Trudy roubou o certificado acima de João Roberto da Silva e alterou o campo e-mail, colocando "trudy@supernet.com.br" para usar a chave pública certificada de João Roberto. Obviamente a Trudy não vai conseguir usar o certificado roubado e adulterado, porque quando um certificado é alterado, o cálculo da/do (I) do novo certificado é (III) da/do (I) referente ao certificado original; isso é garantido pela função SHA-1 utilizada no cálculo da/do (I), como se vê na última linha do certificado acima. A alteração de um bit produz um cálculo (III). Quando um receptor recebe um certificado, ele deve seguir os seguintes passos para validar o certificado:

1. Calcular a/o (I) do certificado recebido, usando a função SHA-1.
2. Decifrar a/o (I) que consta no certificado, utilizando a chave pública da (II).
3. Comparar os cálculos dos passos 1 e 2. Se a/o (I) calculada/o é (III) em comparação com o (I) que consta no certificado após decifragem, este certificado não é válido.

Note que para realizar o passo 2 é preciso ter certeza de estar falando com a (II) correta e que o certificado da (II) de alguma forma é confiável.

As lacunas (I), (II) e (III) são correta e respectivamente preenchidas por uma das seguintes alternativas:

a) chave mestra, sessão, diferente.
b) hash, RSA, igual.
c) hash, Autoridade Certificadora, diferente.
d) chave de sessão, sessão, igual.
e) chave de sessão, Autoridade Certificadora, igual.

Concurso Público para o provimento de vagas em Cargos de Nível Superior da Carreira de Desenvolvimento Tecnológico

CÓDIGO DA VAGA: TP08

9) O que é CA-AFC2?

a) É um conjunto de programas que visam a segurança de computadores;
b) É um conjunto de programas que visam o controle de um cluster de computadores;
c) É um conjunto de programas que visa a eficiência da programação paralela;
d) É um conjunto de programas voltado para a transferência de programas em um ambiente de redes de alto desempenho;
e) É um conjunto de programas que permite gerenciar o desempenho de um computador;

10) Em relação às afirmações abaixo, qual não é verdadeira em relação às vantagens de se usar um servidor tipo "blade"?

a) Ele permite uma maior capacidade de processamento usando um espaço menor de um raque;
b) Ele permite simplificar o cabeamento;
c) Ele proporciona uma redução de consumo em relação a servidores mais antigos;
d) Ele poupa o espaço requerido para sua instalação;
e) Ele permite um melhor gerenciamento de segurança em acessos remotos;

11) Qual é a principal diferença entre as tecnologias "10 gigabit Ethernet" e Ethernet tradicional?

a) A "10 gigabit Ethernet" dispensa o protocolo CSMA/CD;
b) A "10 gigabit Ethernet" usa quadros mínimos e máximos de tamanhos deferentes em relação à Ethernet tradicional;
c) A "10 gigabit Ethernet" consegue suportar alta-velocidade e alta-latência, que são essenciais para um "cluster" de computadores;
d) A "10 gigabit Ethernet" não pode ser usada no contexto das redes convencionais;
e) A "10 gigabit Ethernet" não requer Controle de Acesso ao Meio;

12) Quais dos tópicos seguintes não é coberto no contexto do padrão TIA-942?

a) Arquitetura de rede;
b) Projeto elétrico;
c) Controle do ambiente em que o sistema opera;
d) Proteção contra situações de risco físico;
e) Gerenciamento de dados "off-grid";

13) Quanto ao TCP, é incorreto afirmar que:

a) é um protocolo do nível de transporte.
b) usa janelas deslizantes para implementar o controle de fluxo e erro.
c) é um protocolo orientado a conexão.

d) utiliza portas para permitir a comunicação entre processos localizados em dispositivos diferentes.
e) possui um campo de checksum que valida as informações de seu cabeçalho, mas não valida as informações de payload (campo de dados).

14) Assinale a opção verdadeira sobre o modelo OSI.

a) A camada de enlace de dados é responsável pelo controle do fluxo de dados transmitidos e pela detecção de erros.
b) A camada física junta os bits a transmitir em quadros, e a camada de rede determina qual rota usar até o destino.
c) A camada de sessão é responsável pela gerência dos dados transmitidos, fornecendo mecanismos de formatação, compressão e criptografia.
d) A camada de enlace junta os bits a transmitir e fornece serviços à camada de sessão.
e) A camada de aplicação é responsável pela verificação dos dados transmitidos.

15) Sejam as afirmações:

I) O HTTP e o FTP são protocolos da camada de aplicação e utilizam o protocolo de transporte TCP.
II) Os protocolos HTTP e FTP utilizam duas conexões TCP, uma para controle da transferência e outra para envio dos dados transferidos.
III) O HTTP pode usar conexões não persistentes e persistentes. O HTTP/1.0 usa conexões não persistentes. O modelo default do HTTP/1.1 usa conexões persistentes.
IV) O HTTP é um protocolo sem estado.

Dadas estas três afirmações, indique qual a alternativa correta:

a) I, II e III são verdadeiras.
b) Somente I e II são verdadeiras.
c) Somente I, III e IV são verdadeiras.
d) Somente I e IV são verdadeiras.
e) I, II e III são falsas.

16) Em relação aos sistemas distribuídos, analise as seguintes afirmativas.

I) Um sistema assíncrono apresenta medida de tempo global.
II) A passagem de mensagens é o instrumento empregado para efetuar a comunicação entre os processos de um sistema assíncrono.
III) Em um sistema distribuído transparente quanto à concorrência, a informação de quantos usuários estão utilizando determinado serviço deve ser omitido.
IV) É possível simular um computador paralelo de memória compartilhada usando-se um sistema distribuído.

Concurso Público para o provimento de vagas em Cargos de Nível Superior da Carreira de Desenvolvimento Tecnológico

CÓDIGO DA VAGA: TP08

V) Quando um determinado elemento de um sistema distribuído efetua a difusão de uma mensagem por meio de um multicast, todos os elementos do sistema distribuído recebem a mensagem.

A análise permite concluir que

a) somente a afirmativa V está correta.
b) somente as afirmativas I e II estão corretas.
c) somente as afirmativas I e IV estão corretas.
d) somente as afirmativas II e IV estão corretas.
e) somente as afirmativas I e V estão corretas.

17) Dentre as ferramentas que auxiliam a proteção de um computador, inclui-se o:

a) HTTP.
b) driver do HD.
c) FTP.
d) RSS.
e) antivirus.

18) A técnica de defesa em profundidade é baseada em camadas de segurança. Um dos principais fatores dessa técnica é o perímetro de segurança que forma a borda fortificada de uma rede. O componente do perímetro que utiliza métodos de detecção por anomalia e por assinatura para identificar tráfego malicioso na rede é o

a) IDS
b) Firewall com estado
c) Firewall sem estado
d) Firewall proxy
e) DMZ

19) Dadas as afirmações abaixo sobre segurança de redes:

I) DES, AES e Sha-1 são exemplos de algoritmos criptográficos simétricos.
II) O protocolo de Diffie-Hellman pode ser utilizado para a distribuição de chaves secretas compartilhadas.
III) TLS é um protocolo criptográfico que provê segurança na comunicação pela Internet.

Indique a opção correta:

a) Apenas as afirmações I e II são verdadeiras
b) Apenas as afirmações II e III são verdadeiras
c) Apenas as afirmações I e III são verdadeiras
d) Apenas a afirmação III é verdadeira
e) Todas as afirmações são verdadeiras

Concurso Público para o provimento de vagas em Cargos de Nível Superior da Carreira de Desenvolvimento Tecnológico

CÓDIGO DA VAGA: TP08

20) O SPAM é visto como um grande empecilho no fluxo de E-Mails na Internet. Das diversas técnicas existentes para o controle de SPAM, analise as afirmações abaixo:

I) É recomendável que todo Desktop tenha um cliente de E-Mail e um Firewall configurado de forma a evitar o fluxo de SMTP. O uso de Webmails deve ser cauteloso.

II) Nos servidores, recomenda-se utilizar SMTP autenticado de forma a garantir que apenas usuários reais façam uso do SMTP.

III) O uso de "blacklists" e "whitelists", relacionando endereços IPs e Redes, proporciona um bom filtro de remetentes, eliminando muito SPAM.

IV) A utilização da Biblioteca OpenSSL - SSL/TLS (Secure Sockets Layer/Transport Layer Security) nos servidores de E-Mail é fundamental para eliminar o SPAM.

V) Recomenda-se o uso de Antispam para análise de conteúdo dos E-Mails nos Servidores e nos clientes de E-Mail.

VI) Técnicas de verificação de autenticidade de SMTP, de DNS, verificação de HELO e EHLO, implementadas no servidor, degradam o serviço de E-Mail, congestionam a rede e tornam o fluxo de e-mails inviável.

Indique a opção correta:

a) Apenas as afirmações I e IV são verdadeiras
b) Apenas a afirmação VI é verdadeira
c) As afirmações II, III e V são verdadeiras
d) A afirmação II é falsa
e) As afirmações IV e VI são verdadeiras

Concurso Público para o provimento de vagas em Cargos de Nível Superior da Carreira de Desenvolvimento Tecnológico

CÓDIGO DA VAGA: TP08

QUESTÃO DISCURSIVA

1. **Discuta uma estratégia para garantir confidencialidade, autenticação de remetente e integridade quando do envio de uma mensagem de e-mail.**