INSTITUTO NACIONAL DE PESQUISA ESPACIAL – INPE

PROVA OBJETIVA

TG09

AMBIENTES CRÍTICOS DE TECNOLOGIA DA INFORMAÇÃO EM CENTRO DE DADOS

SUA PROVA

- Além deste caderno contendo **45 (quarenta e cinco)** questões objetivas, você receberá do fiscal de prova o cartão de respostas;
- As questões objetivas têm **5 (cinco)** opções de resposta (A, B, C, D e E) e somente uma delas está correta.

TEMPO

- Você dispõe de **4 (quatro) horas** para a realização da prova;
- **2 (duas) horas** após o início da prova, é possível retirar-se da sala, sem levar o caderno de questões;
- A partir dos **30 (trinta) minutos** anteriores ao término da prova é possível retirar-se da sala **levando o caderno de questões**.

NÃO SERÁ PERMITIDO

- Qualquer tipo de comunicação entre os candidatos durante a aplicação da prova;
- Anotar informações relativas às respostas em qualquer outro meio que não seja no caderno de questões e nas folhas de textos definitivos;
- Levantar da cadeira sem autorização do fiscal de sala;
- Usar o sanitário ao término da prova, após deixar a sala.

INFORMAÇÕES GERAIS

- Verifique se seu caderno de questões está completo, sem repetição de questões ou falhas e também confira seu cargo. Caso tenha recebido caderno de cargo **diferente** do impresso em seu cartão de respostas, o fiscal deve ser **obrigatoriamente** informado para o devido registro na ata da sala;
- Confira seus dados pessoais, especialmente nome, número de inscrição e documento de identidade e leia atentamente as instruções para preencher o cartão de respostas;
- Para o preenchimento do cartão de respostas, use somente caneta esferográfica, fabricada em material transparente, com tinta preta ou azul;
- Assine seu nome apenas no(s) espaço(s) reservado(s) no cartão de respostas;
- Reserve tempo suficiente para o preenchimento do seu cartão de respostas. O preenchimento é de sua responsabilidade e **não será permitida a troca do cartão de respostas em caso de erro cometido pelo candidato**;
- Para fins de avaliação, serão levadas em consideração apenas as marcações realizadas no cartão de respostas;
- A FGV coletará as impressões digitais dos candidatos na lista de presença;
- Os candidatos serão submetidos ao sistema de detecção de metais quando do ingresso e da saída de sanitários durante a realização das provas.

Boa Prova!

FGV CONHECIMENTO

CONHECIMENTOS ESPECÍFICOS

1

A respeito de tipos de virtualização e conceitos de máquinas virtuais, assinale a afirmativa correta.

(A) Na virtualização total de servidor, o hipervisor monitora os recursos do servidor físico, mantendo cada servidor virtual independente e sem conhecimento dos outros servidores virtuais. Nesse tipo de virtualização, não há interação direta do hipervisor com o espaço em disco nem com a unidade de processamento do servidor físico.

(B) A virtualização de rede envolve a abstração de recursos de rede, antes comumente providos de *hardware* para *software*. Essa virtualização permite a segmentação de uma rede física em múltiplas redes virtuais independentes, porém não possui a capacidade de combinar múltiplas redes físicas em uma rede virtual suportada por *software*.

(C) A oferta de *desktops* virtuais para dispositivos endpoint a partir de um data center local ou baseado em nuvem é denominada *Virtual Desktop Infrastructure*. Em ambientes como esse, o sistema operacional do desktop virtual reside no endpoint, não no *datacenter.*

(D) As máquinas virtuais são compostas por somente a aplicação e os arquivos necessários para executá-las. Por serem leves e terem um sistema operacional compartilhado, apresentam facilidade de migração entre diferentes ambientes. Normalmente, possuem tamanho em *megabytes.*

(E) A função de um hipervisor tipo 1 é fornecer suporte a múltiplas réplicas do *hardware* real, isto é, máquinas virtuais, as quais se assemelham aos processos executados por um sistema operacional convencional. Para tal, um hipervisor tipo 1 necessita de uma característica importante: ser executado no modo mais privilegiado da máquina.

2

Com relação à linguagem de marcação de hipertexto (HTML - *HyperText Markup Language*), analise os itens a seguir.

I. O elemento <script> serve para incluir trechos de códigos para serem executados.

II. O elemento <del> serve para incluir comentários no código.

III. O elemento
 não necessita de fechamento.

Está correto o que se afirma em

(A) I, apenas.
(B) II, apenas.
(C) III, apenas.
(D) I e III, apenas.
(E) II e III, apenas.

3

Com relação à linguagem de marcação de hipertexto (HTML - *HyperText Markup Language),* o elemento que representa uma lista de pares de termos e descrições é o

(A) <lt>
(B) <list>
(C) <dt>
(D) <dl>
(E) <dict>

4

Com relação à linguagem de programação JAVA, analise as afirmativas a seguir.

I. Para restringir o acesso de um elemento de uma classe para que seja visível apenas dentro da mesma classe, deve-se usar o modificador de acesso chamado *protected*.

II. Para chamar o construtor da classe herdada (classe base) dentro do construtor da classe derivada da anterior, deve-se usar a instrução s*uper*().

III. Para criar uma variável de referência a um objeto, deve-se usar o operador *new*.

Está correto o que se afirma em

(A) I, apenas.
(B) II, apenas.
(C) III, apenas.
(D) I e II, apenas.
(E) I e III, apenas.

5

Com relação às linguagens de programação C/C++, analise as afirmativas a seguir.

I. Seja x uma variável do tipo inteiro. Na declaração abaixo, o ponteiro p é inicializado com o endereço de x. int *p = &x.

II. O comando *break* somente pode ser utilizado em conjunto com o comando *switch.*

III. O comando *return* encerra a execução de uma função.

Está correto o que se afirma em

(A) I, apenas.
(B) II, apenas.
(C) III, apenas.
(D) I e II, apenas.
(E) I e III, apenas.

6

Com relação à linguagem de programação C++ e o paradigma da orientação a objeto, analise as afirmativas a seguir.

I. Uma classe define o comportamento dos objetos que são instâncias da classe.

II. Em C++ é permitido criar classes derivadas, seguindo o conceito de herança de classes.

III. O polimorfismo permite que objetos de classes diferentes respondam de forma diferente à mesma função.

Está correto o que se afirma em

(A) I, apenas.
(B) II, apenas.
(C) I e II, apenas.
(D) II e III, apenas.
(E) I, II e III.

7

Dockerfile é um arquivo de texto que contém todos os comandos que um usuário pode chamar na linha de comando para montar uma imagem Docker.

Assinale a opção que indica o comando usado para mostrar quais portas a aplicação está escutando.

(A) ENTRYPOINT.
(B) EXPOSE.
(C) ENV.
(D) FROM.
(E) ARG.

8

A respeito de ambientes de máquinas virtuais, *containers* e orquestradores de containers, assinale a afirmativa correta.

(A) *Docker Hub* é uma aplicação *server-side* responsável pelo armazenamento e distribuição de imagens Docker.
(B) O *Kubernetes* recomenda o emprego *de ferramentas externas de garbage collection para complementar o trabalho do kubelet.*
(C) A comunicação entre *Docker Client e Docker Daemon* se dá através da utilização de *web services*, por meio de *sockets* com suporte à XML ou de uma interface de rede.
(D) Os diversos recursos do *kernel Linux* são utilizados pelo *Docker*. Um deles é o *namespaces*, o qual fornece o espaço de trabalho chamado *contêiner,* implementando uma camada de isolamento. Cada aspecto de um *contêiner* é executado em um *namespace* separado e seu acesso é limitado a esse *namespace;*
(E) *Docker Daemon* é um serviço de registro de imagens *Docker* na nuvem, que permite a associação com repositórios para *build* automatizado de imagens.

9

Os sistemas de bancos de dados são fundamentais na organização e gestão de informações em praticamente todos os setores da sociedade moderna. Eles permitem armazenar grandes volumes de dados de forma estruturada, garantindo sua integridade, segurança e acessibilidade.

Assinale a opção que apresenta seus principais componentes.

(A) Uma base de dados, programas de aplicação, o administrador do BD (DBA) e um sistema gerenciador de banco de dados (SGBD).
(B) Um sistema gerenciador de banco de dados (SGBD), *hardware*, banco de dados e usuários.
(C) Um sistema gerenciador de banco de dados (SGBD), linguagem de programação, programas de exploração e base de dados.
(D) Um banco de dados, o administrador do BD (DBA), uma linguagem de programação e um sistema gerenciador de exploração.
(E) Uma base de dados, um sistema gerenciador de banco de dados (SGBD), programas de aplicação/consulta e uma linguagem de exploração.

10

Para que o sistema de banco de dados seja funcional, ele precisa recuperar dados de maneira eficiente. A necessidade de eficiência tem levado os projetistas a usarem estruturas de dados complexas para representar dados no banco de dados. Como muitos usuários de sistema de banco de dados não são treinados em computação, os desenvolvedores ocultam a complexidade dos usuários sob vários níveis de abstração de dados, para simplificar as interações do usuário com o sistema. Com relação à abstração de dados, analise as afirmativas a seguir e assinale (V) para a verdadeira e (F) para a falsa.

( ) O nível lógico descreve em detalhes estruturas de dados complexas de baixo nível.
( ) O nível de visão fornece um mecanismo de segurança de modo a evitar que os usuários acessem certas partes do banco de dados.
( ) O nível físico descreve quais dados estão armazenados no banco de dados e que relações existem entre eles.
( ) O nível lógico descreve o banco de dados inteiro em termos de um pequeno número de estruturas relativamente simples.

As afirmativas são, respectivamente,

(A) F – V – F – V.
(B) V – V – F – V.
(C) V – F – F – V.
(D) V – V – V – F.
(E) F – V – V – F.

11

SQL (*Structured Query Language*) é uma linguagem declarativa padrão usada para gerenciar e manipular bancos de dados relacionais. Ela fornece um conjunto de comandos que permitem aos usuários realizarem diversas operações, como consultar, inserir, atualizar e excluir dados de bancos de dados relacionais.

Relacione as linguagens declarativas às suas respectivas propriedades.

1. DDL – *Data Definition Language*.
2. DML – *Data Manipulation Language*.
3. DTL – *Data Transaction Language*.
4. DCL – *Data Control Language*.

( ) Contém o comando SELECT.
( ) Contém os comandos COMMIT e ROLLBACK.
( ) Utilizada para dar acesso aos usuários.
( ) Contém os comandos CREATE, ALTER e DROP.
( ) Contém os comandos INSERT, UPDATE e DELETE.

Assinale a opção que indica a relação correta, segundo a ordem apresentada.

(A) 1 – 4 – 4 – 1 – 2.
(B) 2 – 3 – 4 – 1 – 2.
(C) 2 – 3 – 3 – 1 – 2.
(D) 3 – 4 – 3 – 2 – 1.
(E) 2 – 3 – 4 – 3 – 1.

12

Os sistemas de arquivos proporcionam uma interface para armazenamento e recuperação de dados em um sistema operacional, cujas implementações podem diferir significativamente em estrutura e funcionalidades.

Em relação aos sistemas de arquivos dos sistemas operacionais, analise as afirmativas a seguir:

I. O sistema NTFS tem como um de seus componentes fundamentais o MFT (*Master File Table*), responsável por armazenar os metadados de todos os arquivos e diretórios presentes em um volume.

II. No sistema ext4, o sistema de arquivos é dividido em grupos de blocos (*Block Groups*), e cada um desses grupos possui seu próprio controle de metadados.

III. O registro de transações (*journaling*) tem como principal objetivo garantir a integridade dos dados e está presente no Linux desde o sistema ext2.

Está correto o que se afirma em

(A) I, apenas.
(B) III, apenas.
(C) I e II, apenas.
(D) II e III, apenas.
(E) I, II e III.

13

Com relação as situações em que a camada de abstração de *hardware* (*HAL*) de um sistema operacional é necessária, analise as afirmativas a seguir.

I. Quando um programador desenvolve um aplicativo sem ter que se preocupar com as características de *hardware* da máquina na qual ele vai ser executado.

II. Quando um aplicativo precisa ser altamente otimizado para um *hardware* específico, sem se preocupar com a portabilidade para outros dispositivos.

III. Quando é necessário acessar recursos de *hardware* específicos de um dispositivo, como sensores e periféricos, de maneira independente do *hardware* subjacente.

Está correto o que se afirma em

(A) I, apenas.
(B) III, apenas.
(C) I e II, apenas.
(D) I e III, apenas.
(E) I, II e III.

14

Em caso de perda ou roubo de um *notebook,* deseja-se que o respectivo sistema operacional ofereça proteção contra o acesso não autorizado aos seus dados.

Neste contexto, considerando um *notebook* com sistema operacional Windows 11 Pro, assinale a opção que indica a ferramenta nativa mais adequada para prover tal proteção.

(A) User Account Control (UAC).
(B) BitLocker.
(C) Windows Security Essentials.
(D) LUKS.
(E) Gerenciador de Credenciais.

15

Sobre os recursos presentes em sistemas operacionais Windows, analise as afirmativas a seguir.

I. No Windows 11, cada processo ou *thread* em execução tem associado a si um *token* de segurança, que carrega a informação sobre identificação e os privilégios do processo ou *thread*.

II. O *Windows Sandbox* é recomendado para a execução de programas que o usuário considera suspeitos ou não confiáveis, pois oferece um ambiente isolado que impede que tais programas afetem o sistema operacional principal.

III. O *Virtualization-Based Security* (*VBS*) é uma tecnologia que visa a executar uma parte do sistema operacional em ambiente virtualizado seguro, e tem como função oferecer acesso remoto ao sistema.

Está correto o que se afirma em

(A) II, apenas.
(B) I e II, apenas.
(C) I e III, apenas.
(D) II e III, apenas.
(E) I, II e III.

16

Uma das tecnologias mais utilizadas no Windows Server é o chamado *pool* de armazenamento (*storage pool*).

Essa tecnologia, baseada nos chamados *storage spaces*, consiste em

(A) áreas de armazenamento designadas para armazenar os dados mais frequentemente acessados, de modo a aumentar a velocidade de acesso.
(B) grupos de discos usados para consolidar *backups* de diversas máquinas virtuais, evitando perda de dados.
(C) uma abstração dos discos físicos existentes em discos virtuais, permitindo uma gestão de armazenamento mais flexível.
(D) uma coleção de serviços de armazenamento em nuvem, com o objetivo de melhorar a velocidade de recuperação de dados.
(E) conjuntos de discos rígidos externos configurados para duplicar dados, de modo a garantir a integridade desses dados.

17

O sistema operacional Android, apesar de ter seu *kernel* baseado no *kernel* Linux, carrega conceitos únicos, voltados à sua aplicação como sistema operacional móvel. Um dos fundamentos do sistema Android é o conceito de *intente.*

Sobre o conceito de *intente,* assinale a afirmativa correta.

(A) É um mecanismo de comunicação restrito a componentes de um mesmo aplicativo.
(B) É um mecanismo de entrega de mensagens entre diferentes partes do sistema Android.
(C) Pode ser classificado como explícitos ou implícitos.
(D) Tem somente a função de inicializar os aplicativos.
(E) Tem o objetivo de reduzir o consumo de memória RAM, limitada pelas características de aparelhos móveis.

18

O *kernel* Linux é composto por diversos subsistemas, onde cada subsistema é responsável por diferentes aspectos do gerenciamento do sistema.

Sobre o *kernel* Linux, analise as afirmativas a seguir.

I. Emprega o chamado *microkernel*, no qual todos os serviços do sistema operacional rodam no espaço do *kernel*.
II. Suporta diferentes sistemas de arquivos, como ext4, NTFS e FAT 32.
III. Suporta o carregamento de módulos em tempo de execução, sem a necessidade de reiniciar o sistema.

Está correto o que se afirma em

(A) II, apenas.
(B) III, apenas.
(C) I e III, apenas.
(D) II e III, apenas.
(E) I, II e III.

19

Tendo em vista a existência de uma vasta gama de distribuições Linux disponíveis, a escolha da distribuição mais adequada para cada usuário ou organização passa pelo conhecimento das necessidades específicas do usuário.

Há uma distribuição Linux em particular que é voltada para profissionais da área de segurança e é considerada a mais avançada quanto a Testes de Penetração (*Pentests*).

Essa distribuição Linux é denominada

(A) Ubuntu.
(B) ArchLinux.
(C) CentOS.
(D) Kali.
(E) Red Hat.

20

Certo programador deseja escrever em uma única linha de comandos um código em Bash que verifica se o valor digitado como entrada é negativo. Caso seja verdade, o código continua em execução, e solicita nova entrada, até que um valor maior ou igual a zero seja digitado.

Nesse caso, é impresso na tela do terminal o número zero e a execução é encerrada. Considere que apenas números inteiros são dados como entrada.

Assinale a opção que apresenta o comando em Bash que executa o desejado.

(A) `while read  n; do if [ n -lt 0 ]; then y=1; else y=0 && break; fi; done; echo y`

(B) `while read  $n; do if [ $n -lt 0 ]; then $y=1; else $y=0 && break; fi; done; echo $y`

(C) `while read  n; do if [ $n -lt 0 ]; then y=1; else y=0 && break; fi; done; echo $y`

(D) `while read $n; do if ( $n -lt 0 ); then y=1; else y=0 && break; fi; done; echo $y`

(E) `while read  n; do if ( n -lt 0 ); then y=1; else y=0 && break; fi; done; echo y`

21

Com relação à programação de *shell scripts*, analise as afirmativas a seguir.

I. Os dois caracteres "#!" quando inseridos no início da primeira linha de um *shell script* servem para indicar o interpretador a ser usado para o programa.
II. Para escrever uma linha de comentário em *bash,* deve-se utilizar o caractere "#" no início da mesma.
III. A linha de comando `a=1 | echo`, escrita em bash, imprime o número 1 na tela do terminal.

Está correto o que se afirma em

(A) I, apenas.
(B) II, apenas.
(C) I e II, apenas.
(D) II e III, apenas.
(E) I, II e III.

22

O Modelo de Referência OSI (*Open Systems Interconnection*) é um modelo de arquitetura em camadas conceitual, aplicado em redes de computadores.

Com relação ao modelo OSI, analise as afirmativas a seguir.

I. A camada de Transporte, ao contrário da camada de Rede, é fim-a-fim, ou seja, liga a origem ao destino.
II. A camada de Rede é responsável pelo controle de erros de transmissão.
III. O modelo OSI abstrai as conexões físicas entre os nós da rede, não possuindo uma camada específica para esse fim.

Está correto o que se afirma em

(A) I, apenas.
(B) I e II, apenas.
(C) I e III, apenas.
(D) II e III, apenas.
(E) I, II e III.

23

O protocolo IP (*Internet Protocol*) é um dos principais protocolos de comunicação em redes de computadores.

Com relação ao endereçamento IPv4 (IP versão 4), analise as afirmativas a seguir.

I. Considerando a máscara de subrede 255.255.128.0, os endereços IPv4 192.168.91.0 e 192.168.48.10 estão na mesma subrede.
II. A faixa de endereços IPv4 referente ao prefixo 124.201.0.0/18 vai de 124.201.0.0 a 124.201.63.255.
III. Todas as interfaces de rede de um mesmo dispositivo possuem o mesmo endereço IPv4.

Está correto o que se afirma em

(A) I, apenas.
(B) II, apenas.
(C) III, apenas.
(D) I e II, apenas.
(E) I e III, apenas.

24

O protocolo TCP (*Transmission Control Protocol*) é responsável pelo controle da transmissão de um fluxo de dados em redes de computadores interligadas.

Com relação ao TCP, analise as afirmativas a seguir.

I. O funcionamento correto do TCP requer o estabelecimento de uma conexão entre a origem e o destino final.

II. O controle de fluxo é implementado por meio de um protocolo do tipo janela deslizante.

III. Todas as conexões TCP são do tipo *full-duplex* e ponto a ponto.

Está correto o que se afirma em

(A) I, apenas.
(B) II, apenas.
(C) I e II, apenas.
(D) II e III, apenas.
(E) I, II e III.

25

As variáveis são uma ferramenta essencial para a programação, as quais permitem armazenar dados definidos apenas na execução, executar e salvar o resultado de operações lógicas e aritméticas, entre outras possibilidades.

A respeito dos diferentes tipos de variáveis que podem ser usadas em um programa, é correto afirmar que

(A) *overflow* e *underflow* não podem ocorrer ao se realizarem operações aritméticas com variáveis do tipo real com representação em ponto-flutuante.
(B) os vetores possuem uma estrutura que permite armazenar uma quantidade pré-definida de variáveis de tipos distintos entre si.
(C) todos os caracteres representados por uma variável do tipo char utilizando codificação ASCII podem ser impressos na tela.
(D) o maior número que um inteiro sem sinal de 8 bits pode representar é 256.
(E) as matrizes são armazenadas de forma contígua na memória.

26

Ao desenvolver códigos profissionais, seguir boas práticas de programação é importante. Seguindo essas práticas, os códigos gerados tendem a ser fáceis de ler, entender e, consequentemente, corrigir e modificar.

Assinale a opção que apresenta uma *boa prática de programação*.

(A) Dar preferência à utilização de variáveis globais ao uso de variáveis locais, caso as últimas necessitem ser passadas como parâmetros para múltiplas funções.
(B) Declarar as variáveis que serão utilizadas no início das suas respectivas funções, separando a declaração das variáveis da lógica do algoritmo em si.
(C) Iniciar todas as linhas do código na primeira coluna à esquerda do editor de texto, visando maximizar à utilização da tela do computador.
(D) Usar nomes curtos para as variáveis, preferencialmente com uma única letra.
(E) Adicionar comentários na maioria das linhas de código do programa.

27

Um ataque do tipo *SQL Injection* consiste na inserção de uma consulta SQL através dos dados de entrada do cliente para a aplicação.

Com relação às defesas primárias recomendadas pela OWASP para esse tipo de ataque, analise as afirmativas a seguir e assinale (V) para a verdadeira e (F) para a falsa.

( ) Implementar *escape* em todos os dados fornecidos pelo usuário.
( ) Emprego de *Stored Procedures* adequadamente construídas.
( ) Utilização de *Prepared Statements* com consultas parametrizadas.

As afirmativas são, respectivamente,

(A) V – F – F.
(B) F – V – V.
(C) F – F – V.
(D) V – V – V.
(E) V – V – F.

28

Servidores que fornecem serviço na internet estão sujeitos a ataques de negação de serviço (DoS), os quais tentam impedir respostas aos clientes por meio da sobrecarga de recursos do servidor. Entretanto, existem determinadas configurações do *Servidor Apache HTTP* que podem ajudar a mitigar esse tipo de problema.

Sobre esse contexto, assinale a afirmativa correta.

(A) A diretiva *TimeOut* deve ser aumentada em *sites* sujeitos a ataques DoS.
(B) Utilizar a diretiva *LoadShare* para distribuir parte do processamento da requisição para sistemas operacionais que permitam essa operação. Tal recurso não está ativo por padrão no *Apache httpd,* mas pode exigir a reconfiguração do seu *kernel*.
(C) A diretiva *MaxRequestWorkers* pode ser reduzida em *sites* sujeitos a ataques DoS. Alguns sites até desativam completamente os *workers* por meio da diretiva *KeepAlive*, o que não gera problemas de desempenho.
(D) A diretiva *RequestReadTimeout* permite implementar ajustes com o objetivo de que o servidor lide com o número máximo de conexões simultâneas sem ficar sem recursos.
(E) O emprego de *threads* via *Multi-Processing Modules* (MPMs) permite trabalhar com mais conexões simultâneas, mitigando assim ataques do tipo DoS.

29

Considere o emprego de TLS (*Transport Layer Security*) para proteger informações trafegadas entre um cliente e um servidor *web*.

Nesse caso, é possível afirmar que o TLS fará uso de

(A) algoritmos de chave simétrica para confidencialidade de dados e códigos de autenticação de mensagens para integridade de dados.
(B) códigos de autenticação de mensagens e algoritmos de chave simétrica para troca de chaves para autenticação.
(C) algoritmos de chave pública para troca de chaves e Diffie-Hellman para integridade de dados.
(D) MD5 ou SHA1 para integridade de dados e algoritmos de chave pública para confidencialidade de dados.
(E) algoritmos de chave pública para confidencialidade de dados e algoritmos de chave simétrica para troca de chaves para autenticação.

30

O fragmento de código a seguir recebe o nome de um arquivo como parâmetro da linha de comando e mostra o seu conteúdo ao usuário. O script é configurado com setuid root, pois visa servir como uma ferramenta educacional para permitir que administradores de sistemas em treinamento examinem arquivos privilegiados do sistema, sem conceder-lhes a capacidade de alterá-los ou causar danos ao sistema.

```
int main(char* argc, char** argv) {
   char cmd[CMD_MAX] = "/usr/bin/cat ";
   strcat(cmd, argv[1]);
   system(cmd);
}
```

Dado que o programa opera com privilégios de administrador, a função *system()* é igualmente executada com tais privilégios. Quando um usuário fornece um nome de arquivo padrão, a chamada funciona como esperado. Contudo, se um invasor inserir uma *string* como ";rm -rf /", a chamada *system()* falhará ao tentar executar o comando "cat" por falta de argumentos, resultando na tentativa subsequente de

(A) excluir recursivamente todo o conteúdo da partição raiz, configurando um ataque do tipo *Denial of Service*.
(B) excluir recursivamente todo o conteúdo da partição raiz, configurando um ataque do tipo *Command Injection*.
(C) copiar recursivamente todo o conteúdo da partição raiz, configurando um ataque do tipo *Direct Dynamic Code Evaluation*.
(D) copiar recursivamente todo o conteúdo da partição raiz, configurando um ataque do tipo *Code Injection*.
(E) excluir recursivamente todo o conteúdo da partição raiz, configurando um ataque do tipo *Man-in-the-middle*.

31

Com base na norma ABNT NBR ISO/IEC nº 27001:2013, sobre a gestão de segurança da informação, assinale a afirmativa correta.

(A) Os indivíduos com responsabilidades atribuídas à segurança da informação não podem transferir as responsabilidades pelas tarefas de segurança da informação para terceiros.
(B) O setor de Tecnologia da Informação é responsável por estabelecer a política de segurança da informação, atribuir responsabilidades e autoridade para garantir a conformidade do Sistema de Gestão da Segurança da Informação (SGSI) com os requisitos da norma.
(C) Após a avaliação de riscos, a próxima etapa deve ser a identificação de uma ou mais contramedidas que possam reduzir os riscos das ameaças identificadas anteriormente. As contramedidas repressivas visam identificar potenciais causadores de um incidente.
(D) É recomendável manter e monitorar adequadamente trilhas de auditoria eletrônicas ou registros físicos para registrar todos os acessos físicos aos ambientes da organização.
(E) A segurança dos recursos humanos envolve a implementação de controles antes, durante e após o processo de contratação, com a definição dos papéis e responsabilidades dos funcionários em relação à segurança da informação realizada durante a contratação.

32

A respeito de segurança em redes de armazenamento do tipo SAN (*Storage Area Networks*), assinale a afirmativa correta.

(A) SANs não são alvos em potencial para invasões, roubo ou uso inadequado de informações devido à sua abrangência e complexidade.
(B) SANs representam redes de infraestrutura que conectam servidores e dispositivos de armazenamento para prover maior segurança, porém com menor eficiência na transmissão de dados.
(C) LUN (*Logical Unit Number*), *Masking* e *Zoning* são os mecanismos básicos de proteção empregados em SANs para evitar acessos não autorizados ao armazenamento.
(D) SANs baseadas em IP oferecem uma segurança natural superior em relação às tradicionais SANs FC (*Fibre Channel*). Isso se deve ao fato de que uma SAN FC é configurada como um ambiente isolado e privado, com uma quantidade maior de nós do que uma rede IP. Portanto, as SANs FC tendem a apresentar mais vulnerabilidades de segurança.
(E) IPSec para extensão SAN via FCIP e filtragem de endereços que não deveriam ser permitidos em sua LAN são estratégias de proteção indicadas para zonas de segurança relacionadas a *Access Control Switch.*

33

Sobre Intrusion Detection Systems (IDS) e Intrusion Prevention Systems (IPS), assinale a afirmativa correta.

(A) Não é uma prática recomendada implantar IPSs em linha para interromper ataques ativamente.
(B) Não é uma desvantagem de IDSs baseados em anomalias serem completamente cegos a novos ataques que ainda não foram registrados.
(C) Um IDS, normalmente situado no limite de rede, realiza uma "inspeção superficial de pacote", analisando somente campos de cabeçalho, não se envolvendo com cargas úteis no datagrama (incluindo dados da camada de aplicação).
(D) São razões pelas quais muitas organizações preferem o uso de IDS ao invés de IPS: ocorrência de tratamento indevido a falsos positivos e gargalo no tráfego da rede.
(E) O IPS é um sistema passivo, limitado a monitorar e gerar alarmes ao detectar atividades suspeitas. Por outro lado, o IDS não só identifica, mas também pode bloquear o tráfego suspeito, adotando uma abordagem mais proativa na prevenção de intrusões.

34

A computação em nuvem proporciona aos usuários acesso a uma capacidade computacional que se adapta à sua demanda, frequentemente superando o que seria economicamente viável adquirir de forma local.

Uma das características que viabiliza a computação em nuvem consiste na abstração dos recursos computacionais físicos dos lógicos.

Essa característica pode ser denominada

(A) elasticidade.
(B) redundância.
(C) escalabilidade.
(D) virtualização.
(E) descentralização.

35

A computação em nuvem trouxe o conceito de "rede como computador", podendo ser dividida em vários modelos de serviço.

Nesse contexto, analise afirmativas a seguir.

I. No modelo IaaS, é possível oferecer ao usuário um serviço para desenvolvimento de aplicativos de modo simplificado, a partir de blocos pré-determinados.
II. No modelo SaaS, os provedores do serviço muitas vezes são os próprios desenvolvedores, o que facilita a customização do aplicativo.
III. Um serviço no modelo PaaS pode ser utilizado para oferecer um serviço do tipo SaaS, ao passo que um serviço no modelo PaaS pode ser desenvolvido através de um serviço do tipo IaaS.

Está correto o que se afirma em

(A) I, apenas.
(B) III, apenas.
(C) I e II, apenas.
(D) II e III, apenas.
(E) I, II e III.

36

Sistemas distribuídos são aqueles em que os recursos de computação, armazenamento e processamento são distribuídos entre vários nós ou dispositivos interconectados por uma rede de computadores. Com relação aos sistemas distribuídos, analise as afirmativas a seguir.

I. São mais fortemente acoplados que multicomputadores.
II. Estão mais suscetíveis a problemas de atrasos e perda de informações.
III. A complexidade dos algoritmos de comunicação aumenta pois há pluralidade de redes e sistemas operacionais envolvidos.

Está correto o que se afirma em

(A) II, apenas.
(B) I e II, apenas.
(C) I e III, apenas.
(D) II e III, apenas.
(E) I, II e III.

37

Um método pelo qual um sistema distribuído pode alcançar alguma medida de uniformidade diante de diferentes sistemas operacionais e hardware subjacente é ter uma camada de software sobre o sistema operacional. Essa camada fornece determinadas estruturas de dados e operações que permitem que os processos e usuários em máquinas distantes operem entre si de uma maneira consistente.

O conceito em questão refere-se a

(A) WANs (*Wide Area Networks*).
(B) *Ethernet*.
(C) *Middleware*.
(D) *Bridge*.
(E) TCP (*Transmission Control Protocol*).

38

Sistemas de tempo real são sistemas que são necessários para computar e entregar resultados corretos dentro de um período de tempo especificado.

Com relação as características comuns de sistemas de tempo real, analise as afirmativas a seguir.

I. São frequentemente orientados por eventos, como sinais de interrupção.
II. São denominados sistemas de tempo real rígido caso a falha em atender aos prazos não cause consequências graves.
III. São projetados para lidar com falhas de forma robusta e devem ser capazes de continuar operando de maneira confiável, mesmo em situações adversas.

Está correto o que se afirma em

(A) I, apenas.
(B) III, apenas.
(C) I e II, apenas.
(D) I e III, apenas.
(E) II e III, apenas.

39

Em relação aos domínios da *camada de enlace*, os diferentes equipamentos de rede podem separar ou não os domínios de colisão e de *broadcast* (difusão) entre suas portas.

Assinale a opção que apresenta o equipamento que originalmente (sem nenhuma configuração avançada) separa tanto o domínio de colisão quanto o de *broadcast.*

(A) *Bridge* (ou ponte).
(B) *Hub* (ou concentrador).
(C) Repetidor.
(D) Roteador.
(E) *Switch* (ou comutador).

40

Um roteador possui em sua tabela de roteamento uma rede delimitada pela máscara IP 255.255.255.240. Excluindo-se os endereços IP de base e de *broadcast*, assinale a opção que indica quantas máquinas podem ser endereçadas nessa rede.

(A) 6.
(B) 8.
(C) 14.
(D) 16.
(E) 30.

41

No Linux, o diretório */etc* contém a maioria dos arquivos básicos de configuração do sistema operacional. O compartilhamento de diretórios locais via *Network File System* (NFS) é um exemplo. Você, como um administrador Linux, pode ser o responsável pelo NFS dos servidores de sua organização. Dessa forma, para configurar o compartilhamento de diretórios locais via NFS, o arquivo a ser usado seria o

(A) bashrc.
(B) export.
(C) mtab.
(D) named.conf.
(E) services.

42

Existem quatro tabelas no *firewall iptables* do Linux, mais uma tabela adicional oriunda do SELinux.

A respeito das tabelas do iptables e suas funcionalidades, analise as afirmativas a seguir e assinale (V) para a verdadeira e (F) para a falsa.

( ) As definições de controle de acesso para pacotes que transitam de, para e através do Linux encontram-se na tabela *filter*.

( ) Na tabela *nat*, é realizada a tradução de endereços de rede. É possível modificar o destino de um pacote por meio de suas regras.

( ) A tabela raw permite modificar os pacotes de acordo com suas regras. Seu uso direto é bastante comum e tem como objetivo alterar a maneira como um pacote é gerenciado.

( ) A tabela *mangle* está presente somente em distribuições Linux com SELinux e permite o bloqueio ou não de um pacote com base em suas políticas, adicionando outra camada de filtragem sobre as regras padrão de filtragem de pacotes.

As afirmativas são, respectivamente,

(A) V – V – F – F.
(B) V – V – F – V.
(C) F – F – V – V.
(D) F – V – F – F.
(E) V – F – F – F.

43

O sistema de arquivos Linux é a estrutura onde são armazenadas todas as informações do computador. Logo, entender como gerenciar o sistema de arquivos a partir do *shell* é uma habilidade crítica para administradores de Linux. Diante disso, acerca de comandos referentes ao sistema de arquivos do Linux assinale a afirmativa correta.

(A) O comando *find* pode ser usado para pesquisar arquivos ou diretórios com base em determinados critérios. No entanto, não pode ser combinado com a opção *delete*, com o objetivo de excluir arquivos.

(B) O comando 'mv $HOME/docs/arq/txt/ $HOME/docs/arq{3,4}' move arq3 e arq4 para o diretório $HOME/docs/arq/txt.

(C) A tentativa de execução do comando 'rm -f $HOME/docs/arq[678]' retorna um erro de sintaxe.

(D) O comando 'chmod -R o-w $HOME/docs' remove recursivamente as permissões de gravação para "outros" em todos os arquivos e diretórios presentes no diretório /docs.

(E) O comando 'cp -R $HOME/docs/* $HOME/tmp' copia todos os arquivos do diretório /docs (inclusive o diretório /docs) assim como todos os arquivos e subdiretórios existentes dentro dele para $HOME/tmp.

44

Você, no papel de administrador de servidores Linux do INPE, necessita conhecer como configurar alguns serviços importantes como DHCP, Proxy, DNS, FTP, etc. A respeito da administração de servidores Linux, analise as afirmativas a seguir e assinale (V) para a verdadeira e (F) para a falsa.

( ) O Linux pode usar um servidor DHCP para obter seu endereço IP, bem como ser configurado para atuar como um servidor DHCP. O serviço mais usado para esse fim é o *Squid,* presente na maioria das distribuições Linux.

( ) O roteamento de pacotes é desabilitado por padrão (ip_forward = 0). Alterando esse valor para 1, o encaminhamento de pacotes é imediatamente habilitado. Para tornar essa alteração permanente, é necessário configurar esse valor ao arquivo /etc/sysctl.conf.

( ) O *bind* é o serviço mais usual da maioria dos servidores profissionais de DNS no Linux. Por padrão, o bind é configurado através da edição do arquivo /etc/named.conf.

As afirmativas são, respectivamente,

(A) F – F – V.
(B) V – F – F.
(C) F – V – F.
(D) V – V – V.
(E) F – V – V.

45

A política de mesma origem é um princípio fundamental de segurança para servidores web. Existe um módulo do Apache HTTP Server que permite que vários usuários hospedem conteúdo na mesma origem. Ao hospedar páginas da web na mesma origem, elas podem ler e controlar umas às outras e problemas de segurança em um site podem se propagar para outros.

A fim de evitar esse tipo de situação, um administrador Linux, ao rodar um servidor Apache, precisa ter cuidado ao utilizar o módulo

(A) mod_auth.
(B) mod_access.
(C) mod_userdir.
(D) mod_vhost_alias.
(E) mod_cgi.

Realização