Sistemas Operacionais 2025.2 – Lista de Exercícios 2

Tratamento de Entrada e Saída (E/S)

1. Em relação às camadas de software de E/S, qual camada é responsável por enviar comandos diretos ao hardware do controlador de dispositivo?

a) Software de E/S de espaço de usuário.

b) Software de E/S independente do dispositivo.

c) Drivers de dispositivo.

d) Camada de interrupções.

e) Biblioteca de E/S padrão.

2. Qual das seguintes afirmações descreve corretamente o acesso a dispositivos de E/S mapeados na memória (memory-mapped I/O)?

a) Os dispositivos de E/S possuem um espaço de endereços separado que a CPU acessa com instruções especiais de E/S.

b) Os registradores do controlador de dispositivo são acessados como se fossem locais de memória comum, utilizando as mesmas instruções de carregamento e armazenamento da CPU.

c) A CPU não pode acessar diretamente os dispositivos de E/S, dependendo inteiramente do DMA.

d) Apenas a memória de vídeo pode ser mapeada na memória principal.

e) É uma técnica utilizada exclusivamente para dispositivos de rede de alta velocidade.

3. O que é um "driver de dispositivo" em um sistema operacional moderno?

a) Um programa de usuário que solicita operações de E/S.

b) Uma parte do kernel que gerencia a comunicação específica com um tipo de hardware de E/S.

c) O hardware físico que controla um dispositivo periférico.

d) Um buffer de memória usado para operações de E/S.

e) A interface gráfica do usuário para dispositivos periféricos.

4. Em um sistema com E/S programada (programmed I/O), qual é a principal desvantagem em termos de desempenho da CPU?

a) O controlador de dispositivo precisa de permissão da CPU para cada byte transferido.

b) A CPU é constantemente interrompida pelo controlador de dispositivo a cada transferência de byte.

c) A CPU fica em um "loop de espera" (polling) ou é interrompida a cada byte transferido, consumindo muitos ciclos de CPU.

d) O DMA assume todas as transferências, sobrecarregando o barramento.

e) É necessário um software de E/S de espaço de usuário muito complexo para gerenciar as operações.

Sistemas de Arquivos

5. Qual a função de um diretório em um sistema de arquivos?

a) Armazenar os blocos de dados reais dos arquivos.

b) Conter os metadados dos arquivos (i-nodes).

c) Mapear nomes de arquivos para seus respectivos i-nodes (ou outras estruturas de metadados) e organizar os arquivos em uma estrutura hierárquica.

d) Gerenciar o espaço livre no disco.

e) Proteger os arquivos contra acesso não autorizado.

6. Em um sistema de arquivos UNIX/Linux, o que é um "link simbólico" (soft link)?

a) Uma cópia exata de um arquivo, ocupando novo espaço em disco.

b) Um ponteiro direto para os blocos de dados de um arquivo.

c) Um arquivo que contém o caminho para outro arquivo, e seu i-node é diferente do arquivo original.

d) Um link que aponta para o mesmo i-node do arquivo original.

e) Um atalho que só funciona dentro do mesmo diretório.

7. O que é fragmentação interna em um sistema de arquivos?

a) Ocorre quando os arquivos são armazenados em blocos não contíguos no disco.

b) Refere-se ao espaço não utilizado dentro do último bloco alocado para um arquivo, pois o arquivo não preenche o bloco inteiro.

c) A incapacidade de alocar um arquivo grande devido à dispersão do espaço livre.

d) O resultado da exclusão de muitos arquivos pequenos.

e) É a redundância de dados em um sistema de arquivos distribuído.

8. No contexto de alocação de arquivos em disco, qual a principal vantagem da alocação encadeada (linked allocation)?

a) Permite acesso direto (aleatório) rápido aos blocos de dados de um arquivo.

b) É muito eficiente para arquivos pequenos, pois minimiza o overhead de ponteiros.

c) Evita completamente a fragmentação externa, pois os arquivos podem usar qualquer bloco livre disponível.

d) Garante que os arquivos sejam armazenados em blocos contíguos para maximizar o desempenho.

e) Permite uma recuperação de falhas mais robusta em caso de corrupção.

Sistemas com Múltiplos Processadores

9. Em um sistema multiprocessador SMP, como o sistema operacional lida com a execução de um processo que requer acesso exclusivo a uma seção crítica?

a) O processo é pausado indefinidamente até que todos os outros processadores estejam ociosos.

b) O sistema operacional atribui a seção crítica a um único processador e impede que os outros a acessem.

c) Utiliza mecanismos de sincronização (como locks ou semáforos) para garantir que apenas um processador por vez execute a seção crítica.

d) Duplica a seção crítica em cada cache de CPU para que todos possam acessá-la simultaneamente.

e) Converte o processo em uma thread leve para evitar problemas de concorrência.

10. Qual a principal motivação para o uso de sistemas multiprocessadores em vez de sistemas de CPU única cada vez mais rápidos?

a) A dificuldade física e os limites de dissipação de calor para aumentar continuamente a frequência de um único processador.

b) O menor custo de produção de múltiplos processadores de menor desempenho.

c) A simplificação do desenvolvimento de software paralelo.

d) A melhoria automática do desempenho de software sequencial.

e) A necessidade de isolar completamente as aplicações umas das outras.

11. Em sistemas multiprocessadores, o que é um "spinlock" e qual sua principal desvantagem?

a) Um tipo de semáforo que coloca o processo em espera quando o recurso está ocupado.

b) Um lock que faz um processador ficar em um loop ocupado ("spinning") verificando repetidamente se o recurso foi liberado, consumindo ciclos de CPU desnecessariamente se o lock for mantido por muito tempo.

c) Uma técnica de interrupção que paralisa temporariamente todos os outros processadores.

d) Um método de cache para sincronizar dados entre múltiplas CPUs.

e) Uma primitiva de hardware para garantir a atomicidade de operações.

12. Qual é a finalidade de um mecanismo de barramento (bus) em um sistema multiprocessador SMP?

a) Conectar a CPU diretamente ao disco rígido.

b) Fornecer um caminho de comunicação compartilhado para que CPUs, memória e dispositivos de E/S possam trocar dados.

c) Gerenciar a distribuição de tarefas entre os diferentes processadores.

d) Atuar como um switch para controlar o fluxo de energia.

e) Isolar completamente um processador do outro para evitar interferência.

Proteção e Segurança

13. O que define a "política de segurança" em um sistema operacional?

a) O mecanismo de hardware que impõe as regras de segurança.

b) A decisão sobre "o que" deve ser protegido e "quem" deve ter permissão para fazer "o quê".

c) O conjunto de técnicas de criptografia usadas para proteger dados.

d) O software antivírus instalado no sistema.

e) O processo de auditoria e registro de eventos de segurança.

14. No modelo de proteção, qual o objetivo da "matriz de acesso"?

a) Armazenar informações sobre a conectividade de rede do sistema.

b) Descrever formalmente os direitos de acesso de cada sujeito (domínio/processo) a cada objeto (recurso) no sistema.

c) Gerenciar a alocação de memória virtual para os processos.

d) Registrar as falhas do sistema para depuração.

e) Mapear endereços lógicos para endereços físicos.

15. O que é "Privilégio Mínimo" como princípio de segurança?

a) Conceder a todos os usuários acesso irrestrito, confiando em sua ética.

b) Conceder a cada usuário ou processo apenas as permissões e recursos estritamente necessários para realizar sua tarefa designada e nada mais.

c) Minimizar a quantidade de software de segurança instalado no sistema.

d) Permitir que usuários com privilégios de administrador acessem todos os recursos sem restrições.

e) Ignorar permissões de arquivos para acelerar o acesso.

16. Qual o objetivo de um "sistema de detecção de intrusão" (IDS - Intrusion Detection System)?

a) Impedir completamente todas as tentativas de acesso não autorizado à rede.

b) Monitorar o tráfego de rede e/ou atividades do sistema em busca de padrões que indiquem ataques ou comportamento malicioso.

c) Criptografar automaticamente todos os dados sensíveis do sistema.

d) Realizar backups diários de todos os arquivos do sistema.

e) Gerenciar a autenticação e autorização de usuários.

17. O que é "engenharia social" no contexto de segurança da informação?

a) Uma técnica de programação para desenvolver software seguro.

b) A manipulação psicológica de pessoas para que elas revelem informações confidenciais ou realizem ações que comprometam a segurança.

c) O uso de algoritmos complexos para quebrar senhas.

d) A criação de programas de computador que exploram vulnerabilidades técnicas.

e) O estudo das interações entre sistemas operacionais e usuários.

18. Qual o papel de um "módulo de segurança de hardware" (HSM - Hardware Security Module)?

a) Executar o sistema operacional em um ambiente virtualizado.

b) Prover um ambiente seguro para armazenamento de chaves criptográficas e execução de operações criptográficas sensíveis.

c) Acelerar o processamento gráfico de um sistema.

d) Gerenciar a alocação de memória RAM para aplicações.

e) Controlar a interface de usuário de dispositivos periféricos.

19. O que é um ataque de "negação de serviço" (DoS - Denial of Service)?

a) Um ataque que rouba informações confidenciais de um servidor.

b) Um ataque que visa tornar um serviço ou recurso de rede inacessível aos usuários legítimos, sobrecarregando-o.

c) Um ataque que criptografa os dados de um sistema e exige um resgate.

d) Um ataque que instala software malicioso para monitorar a atividade do usuário.

e) Um ataque que modifica as permissões de acesso a arquivos no sistema.

20. Por que o princípio de "Defesa em Profundidade" é importante para a segurança do sistema?

a) Garante que apenas uma camada de segurança seja suficiente para proteger o sistema.

b) Baseia-se na implementação de múltiplas camadas de segurança independentes, de modo que a falha de uma não comprometa a segurança total.

c) Foca exclusivamente na proteção do perímetro da rede.

d) Sugere que a melhor defesa é um ataque preventivo contra invasores.

e) Reduz a complexidade do sistema de segurança para facilitar a manutenção.
