Edital de Seleção 061/2025 PROPESP/UFAM

Prova de Conhecimento

Caderno de Questões

Nome do Candidato: _____

_____
Assinatura do Candidato conforme identidade

INSTRUÇÕES PARA O CANDIDATO:

- Verifique o seu nome e o número da sua inscrição impressos neste CADERNO DE QUESTÕES. Assine seu nome no local apropriado somente quando autorizado pelo aplicador da prova, no momento da identificação.
- As respostas a todas questões devem ser preenchidas na FOLHA DE RESPOSTAS, no campo correspondente a cada questão.
- Em nenhuma hipótese haverá substituição deste CADERNO DE QUESTÕES por erro de preenchimento do candidato.
- Este CADERNO DE QUESTÕES ficará disponível aos candidatos a partir do dia 27/09/2025, após as 15h no site do projeto.

QUESTÃO 01. Considere um sistema que exige o armazenamento de dados sensíveis, onde a integridade da informação é crucial e a possibilidade de alteração acidental é inaceitável. Qual das seguintes abordagens seria a mais apropriada para garantir que o valor não seja modificado após sua inicialização?

a) Declarar a informação como uma variável global para facilitar o acesso e a manipulação em diferentes funções.
b) Declarar a informação como uma constante para que o compilador imponha a imutabilidade, gerando um erro se houver uma tentativa de reatribuição.
c) Armazenar a informação em uma variável, mas implementando uma estrutura condicional (if) para checar e reverter qualquer alteração.
d) Utilizar um tipo de dado primitivo (como um inteiro ou string), pois em algumas linguagens esses tipos são tratados como imutáveis quando declarados como constantes.
e) Utilizar uma estrutura de dados de lista ou vetor para armazenar o valor, pois essa estrutura permite controle de acesso indexado, embora não impeça a reatribuição de elementos.

QUESTÃO 02. Analise o seguinte trecho de código e determine o valor final da variável resultado. Considere que a linguagem utilizada reconhece os operadores relacionais e lógicos (and, or, not) como válidos, e que a precedência dos operadores segue o padrão: aritméticos > relacionais > lógicos.

```
int x = 10;
bool resultado = (x * 2 > 15) and (x % 3 == 1);
```

a) Um erro de compilação, pois a sintaxe está incorreta.
b) 15
c) true
d) false
e) 1

QUESTÃO 03. Em um sistema de autenticação, o desenvolvedor utiliza um tipo de dado inteiro sem sinal de 8 bits (faixa de 0 a 255) para armazenar o número de tentativas de login de um usuário. Considerando que a cada tentativa falha o contador é incrementado em 1 e que a linguagem de programação utilizada permite o wrap-around em caso de overflow (comportamento típico em C/C++ para tipos unsigned), qual risco de segurança pode surgir dessa escolha de tipo de dado?

a) Pode ocorrer um integer overflow, permitindo que um invasor resete o contador de tentativas para zero.
b) A falta de um sinal (sem sinal) impede que o valor seja decrementado corretamente.
c) O tipo de dado inteiro não pode armazenar valores negativos, o que limita sua utilidade.
d) O tipo de dado é muito grande e consome recursos desnecessários.
e) É mais lento para processar do que um tipo de dado de ponto flutuante, criando um gargalo de desempenho.

QUESTÃO 04. Um desenvolvedor está criando um módulo de validação de dados de entrada para evitar ataques de injeção de SQL. Qual das seguintes práticas é a mais eficaz para prevenir esse tipo de ataque?

a) **Validar entradas usando instruções condicionais para verificar palavras-chave SQL.**
b) Utilizar prepared statements com parametrização de consultas.
c) Empregar laços de repetição para filtrar caracteres especiais manualmente.
d) Aplicar comandos de desvio para ignorar entradas suspeitas.
e) Configurar um firewall de aplicação (WAF) como única medida de proteção.

QUESTÃO 05. Considerando o princípio de modularização, qual das seguintes práticas seria a mais segura em um projeto de software, visando a minimização de vulnerabilidades de segurança?

a) Criar funções de uso geral que não têm uma responsabilidade de segurança específica para evitar erros de implementação.
b) Criar um módulo de validação de dados com acesso irrestrito a partir de qualquer parte do sistema, sem controle de escopo.
c) Manter todas as funções de segurança (autenticação, criptografia) em um único módulo para fácil acesso e gerenciamento.
d) **Encapsular funções com responsabilidades de segurança bem definidas em módulos separados, acessando-os apenas quando necessário.**
e) Evitar a criação de funções para criptografia e validação, implementando o código diretamente onde for necessário para evitar dependências.

QUESTÃO 06. Em um sistema de autenticação, senhas de usuários nunca devem ser armazenadas em texto puro no banco de dados. Em vez disso, utilizam-se funções de hash criptográficas (como bcrypt, PBKDF2 ou Argon2). Qual é a principal razão para essa prática?

a) O hash é mais rápido de ser verificado do que uma senha em texto puro.
b) **O hash impede que invasores que acessem o banco de dados obtenham as senhas originais dos usuários, devido à irreversibilidade da função.**
c) O hash permite que a senha seja recuperada pela equipe de suporte em caso de esquecimento.
d) O hash reduz o espaço de armazenamento necessário para as senhas.
e) O hash previne que as senhas sejam alteradas por usuários não autorizados.

QUESTÃO 07. No modelo OSI, em que camada um ataque de envenenamento de cache ARP (ARP Spoofing) ocorre, e por que ele é uma ameaça à segurança?

a) Camada 1 (Física), porque interfere diretamente nos sinais elétricos da rede.
b) Camada 4 (Transporte), pois afeta o estabelecimento de conexões TCP/UDP.
c) Camada 3 (Rede), porque altera o endereço de roteamento dos pacotes.
d) Camada 7 (Aplicação), porque manipula o conteúdo das requisições HTTP.
e) **Camada 2 (Enlace), pois falsifica o mapeamento entre endereços MAC e endereços IP, redirecionando o tráfego da rede.**

QUESTÃO 08. Um administrador de rede precisa configurar um firewall para bloquear todo o tráfego de entrada, exceto para o serviço web na porta 443. Que modelo de segurança de firewall ele está implementando e qual o protocolo relacionado à porta 443?

a) Política de "allow by default"; protocolo FTP.
b) Política de "deny all, permit only explicit exceptions"; protocolo HTTPS.
c) Política de "block by content"; protocolo HTTP.
d) Política de "permit all, block explicit exceptions"; protocolo HTTP.
e) Política de "stateful inspection"; protocolo HTTPS.

QUESTÃO 09. Um ataque de spoofing de IP (falsificação de endereço de origem) é frequentemente utilizado para ocultar a origem de ataques DDoS. No contexto de prevenção, qual característica do protocolo IPv6 — em contraste com o IPv4 — facilita significativamente a implementação de mecanismos anti-spoofing, como o Reverse Path Forwarding (RPF), tornando mais difícil a falsificação bem-sucedida de endereços?

a) O espaço de endereçamento extremamente amplo, que reduz drasticamente a possibilidade de um atacante adivinhar ou forjar um endereço fonte válido e roteável.
b) A simplificação do cabeçalho, que agiliza a inspeção de pacotes pelos roteadores.
c) A eliminação da necessidade de NAT, o que simplifica o rastreamento de origem.
d) A capacidade de criar sub-redes menores e mais segmentadas.
e) O suporte nativo ao IPsec para autenticação e criptografia.

QUESTÃO 10. Em uma arquitetura de microsserviços bem projetada, se um invasor compromete um único serviço, qual é a principal vantagem de segurança em comparação com uma arquitetura monolítica?

a) A arquitetura de microsserviços não oferece vantagens de segurança inerentes.
b) O comprometimento de um serviço pode levar a uma falha em cascata, anulando qualquer vantagem.
c) O princípio de isolamento contém a violação ao serviço afetado, impedindo que outros serviços sejam diretamente comprometidos.
d) A heterogeneidade de tecnologias dificulta a exploração de vulnerabilidades comuns.
e) A implantação independente permite correções mais rápidas, mas não isola o impacto de um ataque.

QUESTÃO 11. Um ataque buffer overflow em um programa é uma vulnerabilidade de segurança que pode ser explorada para injetar código malicioso. Qual dos seguintes componentes de arquitetura de computador é o mais diretamente afetado por esse tipo de ataque?

a) O sistema de I/O, que pode ser redirecionado para enviar dados a um destino não autorizado.
b) O pipeline de instruções da CPU, que causa um stall e permite a injeção do código.
c) A unidade de controle da CPU, que interpreta instruções malformadas como válidas devido à corrupção do fluxo de execução.
d) O cache de dados, que pode ser envenenado para fornecer dados incorretos à CPU.
e) **A memória (RAM), pois o ataque sobrecarrega um buffer na stack ou no heap, permitindo a execução de código arbitrário.**

QUESTÃO 12. O que é um handshake TCP e qual é a sua importância em um contexto de segurança de rede?

a) **É um processo de três vias (SYN, SYN-ACK, ACK) para estabelecer uma conexão confiável. Um ataque de SYN flood explora esse processo para exaurir os recursos do servidor.**
b) É um mecanismo de controle de fluxo de dados que impede que o buffer do servidor seja sobrecarregado por pacotes maliciosos.
c) É um protocolo de verificação de integridade de pacotes que garante que nenhum dado foi alterado durante a transmissão.
d) É um processo de criptografia de pacotes em que a chave de criptografia é trocada entre o cliente e o servidor.
e) É uma sequência de três pacotes (SYN, SYN-ACK, ACK) para estabelecer uma conexão segura e autenticar as partes.

QUESTÃO 13. Um administrador de sistema precisa conceder a um usuário a capacidade de ler e executar arquivos de um diretório, mas não de modificá-los. Em um sistema de arquivos Linux, que permissões seriam mais adequadas e qual é a representação numérica octal correspondente?

a) Permissões 'leitura', 'escrita' e 'execução'; 7
b) Permissões 'leitura' e 'escrita'; 6
c) **Permissões 'leitura' e 'execução'; 5**
d) Permissões 'somente leitura'; 4
e) Não é necessário atribuir permissões específicas, pois o usuário herda as permissões do grupo por padrão.

QUESTÃO 14. Um analista de segurança usa o Wireshark e observa um grande volume de pacotes SYN vindos de um único IP de origem para um único IP de destino, mas em diversas portas aleatórias. O servidor destino apresenta lentidão e incapacidade de estabelecer novas conexões legítimas. Que tipo de ataque é esse e qual é o seu objetivo?

a) Ataque de IP spoofing para ocultar a origem.
b) Ataque de SYN Flood com o objetivo de realizar um port scan.
c) Ataque de Port Scan para mapear serviços abertos.
d) **Ataque de SYN Flood com o objetivo de negar o serviço (DoS).**
e) Ataque de Man-in-the-Middle para interceptar sessões.

QUESTÃO 15. Em um sistema operacional, o kernel tem um papel fundamental na segurança do sistema. Qual das seguintes funções é uma responsabilidade de segurança do kernel?

a) Monitorar o uso de aplicativos de terceiros para garantir a conformidade.
b) Prover conectividade à internet para todos os aplicativos.
c) **Garantir o isolamento entre processos e controlar o acesso à memória e aos recursos do sistema.**
d) Gerenciar a interface gráfica do usuário (GUI).
e) Executar o pipeline de instruções da CPU para otimizar o desempenho.

QUESTÃO 16. Um ataque de injeção de código, como SQL injection, é uma das vulnerabilidades mais comuns em aplicações web. Qual componente backend é o alvo final desse tipo de ataque?

a) O load balancer, pois ele distribui as requisições maliciosas.
b) O frontend, que renderiza o conteúdo injetado.
c) O banco de dados, pois a consulta injetada é executada nele, comprometendo a integridade dos dados.
d) O servidor de cache, pois armazena respostas contaminadas.
e) O sistema de gerenciamento de processos, que é sobrecarregado pelas consultas maliciosas.

QUESTÃO 17. O ping é uma ferramenta de rede usada para verificar a conectividade. Em um cenário de cibersegurança, qual é a principal limitação do ping para um analista de segurança, e que tipo de ataque pode ser usado para falsificar a resposta do ping?

a) O ping não verifica se um serviço específico (ex.: HTTP) está ativo, apenas a conectividade de rede; ataques de spoofing de ICMP.
b) O ping não funciona em redes IPv6; ataques de DNS spoofing.
c) O ping consome muitos recursos de rede; ataques de SYN flood.
d) O ping não criptografa suas mensagens; ataques de man-in-the-middle.
e) O ping não diferencia entre hosts físicos e virtuais; ataques de ARP spoofing.

QUESTÃO 18. Um firewall de aplicação (WAF) é uma ferramenta de segurança que opera em qual camada do modelo OSI e qual é o seu principal objetivo em cibersegurança?

a) Camada 2 (Enlace); proteger contra ataques de ARP spoofing.
b) Camada 4 (Transporte); filtrar portas e protocolos como TCP e UDP.
c) Camada 5 (Sessão); gerenciar sessões de usuários para evitar session hijacking.
d) Camada 7 (Aplicação); proteger aplicações web contra ataques como SQL injection e XSS.
e) Camada 3 (Rede); bloquear endereços IP maliciosos.

QUESTÃO 19. Em um ambiente de virtualização, o hypervisor é um componente crítico de segurança. Qual é o seu papel principal e por que ele é importante para a segurança do ambiente virtualizado?

a) Ele é um sistema de monitoramento de rede que impede ataques de buffer overflow.
b) Ele é o gerenciador de recursos que isola as máquinas virtuais umas das outras, garantindo que uma falha em uma não afete as outras.
c) Ele é um firewall que protege a comunicação entre as máquinas virtuais.
d) Ele é um sistema de backup que garante que as máquinas virtuais possam ser recuperadas em caso de ataque.
e) Ele é o sistema operacional da máquina virtual e isola o acesso à memória.

QUESTÃO 20. O protocolo HTTPS adiciona segurança ao HTTP por meio da implementação de um protocolo subjacente que opera entre as camadas de Transporte e Aplicação. Qual é o nome desse protocolo e a sua função primordial?

a) O protocolo IPsec, que opera na camada de Rede para criptografar pacotes individualmente e garantir a autenticidade dos endereços IP.
b) O protocolo TLS/SSL, cuja função primordial é autenticar a identidade do usuário final perante a aplicação web, utilizando certificados digitais para validar suas credenciais de login.
c) O protocolo TLS/SSL, cuja função primordial é atuar como um firewall de aplicação, inspecionando o conteúdo do tráfego HTTP em busca de ataques como SQL Injection ou Cross-Site Scripting (XSS) e bloqueando-os.
d) O protocolo TLS/SSL, cuja função é estabelecer um canal seguro para garantir a confidencialidade e a integridade dos dados.
e) O protocolo OAuth 2.0, que gerencia a autorização e a delegação de acesso a recursos por meio de tokens, garantindo que apenas usuários autenticados acessem a aplicação.

QUESTÃO 21. Um administrador de sistema está configurando as permissões de acesso a um arquivo de log crítico em um sistema Linux. Qual é a prática mais segura, com base no princípio de privilégio mínimo?

a) Definir apenas permissão de leitura para o proprietário, apenas permissão de leitura para o grupo de administradores e sem permissão para outros.
b) Conceder permissões de leitura e escrita para o grupo específico de administradores e permissões de somente leitura para o proprietário do arquivo.
c) Definir as permissões como somente leitura para o proprietário e sem permissão para outros usuários e grupos.
d) Não definir nenhuma permissão, pois o sistema operacional gerencia automaticamente o acesso seguro.
e) Conceder permissões de leitura, escrita e execução para todos os usuários.

QUESTÃO 22. Em sistemas distribuídos, mecanismos de sincronização mal implementados podem introduzir falhas que comprometem a segurança. Qual dos seguintes mecanismos, se implementado incorretamente, pode ser mais facilmente explorado por um atacante para causar uma condição de negação de serviço (DoS) de forma previsível?

a) Comunicação por passagem de mensagens assíncrona, pois a perda de mensagens pode exigir retransmissão, consumindo recursos de rede.
b) Relógios lógicos de Lamport, pois a dessincronização pode causar inconsistências na ordem de eventos, levando a comportamentos inesperados da aplicação.
c) Protocolos de tolerância a falhas bizantinas, pois sua complexidade computacional pode ser explorada para sobrecarregar os nós consensuais.
d) Semáforos ou mutexes distribuídos, pois um atacante pode manipular a ordem de aquisição de recursos para induzir um deadlock, paralisando permanentemente os processos envolvidos até uma intervenção manual.
e) Barreiras de sincronização, pois um atacante pode impedir que um processo chegue à barreira, fazendo com que os demais processos fiquem bloqueados indefinidamente aguardando.

QUESTÃO 23. O que é um rootkit e qual é a principal camada do sistema operacional que ele ataca para permanecer indetectável?

a) É um tipo de malware que ataca a Camada de Aplicação e manipula os dados do usuário para roubar informações.
b) É um ataque de negação de serviço que inunda o sistema com requisições maliciosas.
c) É um conjunto de ferramentas que manipula o kernel do sistema operacional para esconder a presença de um atacante, tornando-o indetectável por ferramentas de segurança de nível de usuário.
d) É um tipo de malware que ataca a Camada de Abstração de Hardware e manipula os drivers para controlar o sistema.
e) É um script malicioso que ataca a memória stack e causa um buffer overflow.

QUESTÃO 24. Em sistemas distribuídos, a comunicação entre os microsserviços pode ser um ponto de vulnerabilidade. Qual das seguintes práticas de segurança é a mais eficaz para proteger a comunicação entre os microsserviços?

a) Usar o protocolo HTTP para a comunicação entre os serviços.
b) Usar a API gateway para controlar o acesso aos serviços.
c) Usar um message queue para a comunicação assíncrona.
d) Usar um firewall para filtrar o tráfego entre os serviços.
e) Criptografar toda a comunicação usando o protocolo TLS e implementar a autenticação mútua entre os serviços.

QUESTÃO 25. Um ataque de ransomware bem realizado é capaz de criptografar os arquivos de uma organização e torná-los inacessíveis. Qual dos três pilares da Tríade CIA (Confidencialidade, Integridade, Disponibilidade) é o mais diretamente afetado neste cenário por este tipo de ataque?

a) Integridade, porque os dados são modificados.
b) Disponibilidade, porque os usuários perdem o acesso aos seus dados e sistemas.
c) Ataques de ransomware afetam todos os três pilares da Tríade CIA, mas não de forma direta.
d) Confidencialidade e Integridade, mas não a Disponibilidade.
e) Confidencialidade, porque os dados podem ser roubados e divulgados.

QUESTÃO 26. O que a norma ISO/IEC 27001 define e qual a sua importância para a gestão de segurança da informação em uma organização?

a) Define uma política de uso aceitável da internet para os funcionários.
b) Define um conjunto de ferramentas e tecnologias de segurança que devem ser utilizadas.
c) Define as penalidades legais para violações de dados, como o GDPR.
d) Define os requisitos para a realização de auditorias de segurança, mas não a implementação dos controles.
e) Define um SGSI (Sistema de Gestão de Segurança da Informação), fornecendo uma estrutura para a proteção de informações confidenciais.

QUESTÃO 27. A criptografia simétrica é amplamente utilizada para criptografar grandes volumes de dados devido ao seu desempenho. Qual afirmação descreve corretamente a característica fundamental que define a criptografia simétrica e a diferencia da criptografia assimétrica?

a) Ela é menos segura que a criptografia assimétrica, mas significativamente mais rápida para operações com grandes volumes de dados.
b) Ela utiliza um par de chaves distintas: uma chave pública para criptografia e uma chave privada para descriptografia.
c) Ela utiliza exatamente a mesma chave secreta compartilhada entre as partes para realizar tanto a criptografia quanto a descriptografia dos dados.
d) A segurança do esquema depende totalmente da complexidade do algoritmo, pois a chave é sempre pública e conhecida.
e) Sua principal aplicação é gerar assinaturas digitais para garantir autenticidade e não-repúdio.

QUESTÃO 28. A criptografia assimétrica é utilizada para garantir a confidencialidade e a integridade em comunicações. Qual é o papel da chave pública e da chave privada em um processo de criptografia e descriptografia de dados?

a) Apenas a chave privada é usada para criptografar e descriptografar, e a chave pública é usada apenas para autenticação.
b) A chave pública é usada para criptografar os dados, e a chave privada correspondente é usada para descriptografá-los.
c) A chave privada é usada para criptografar, e a chave pública é usada para descriptografar.
d) Ambas as chaves são usadas para criptografar os dados.
e) A chave pública é usada para descriptografar, e a chave privada é usada para criptografar.

QUESTÃO 29. Uma assinatura digital é um mecanismo de segurança essencial para garantir a autenticidade e o não-repúdio de um documento digital. Qual par de chaves é usado para assinar um documento e para verificar a assinatura, respectivamente?

a) A chave pública do receptor para assinar, e a chave privada do emissor para verificar.
b) A chave privada do emissor para assinar, e a chave privada do receptor para verificar.
c) A chave privada do emissor para assinar, e a chave pública do emissor para verificar.
d) A chave pública do emissor para assinar, e a chave privada do emissor para verificar.
e) A chave pública do receptor para assinar, e a chave privada do emissor para verificar.

QUESTÃO 30. Um ataque de engenharia social é uma técnica de ataque que explora a psicologia humana para enganar as vítimas. Qual dos seguintes controles de segurança seria mais eficaz para mitigar um ataque de engenharia social?

a) A realização de treinamentos de conscientização de segurança para os funcionários.
b) Um IDS/IPS, pois ele pode detectar o comportamento malicioso do atacante.
c) Um firewall de rede, pois ele pode bloquear o tráfego do atacante.
d) O uso de criptografia para proteger os dados confidenciais.
e) A aplicação de patches de segurança, que corrige vulnerabilidades de software.

QUESTÃO 31. Firewalls e sistemas IDS/IPS (Intrusion Detection/Prevention System) são componentes essenciais de uma arquitetura de segurança de rede. Considerando suas funções conceituais primárias, qual afirmação descreve corretamente a distinção fundamental entre eles?

a) O firewall atua primariamente como uma ferramenta de detecção de ameaças baseada em assinaturas, enquanto o IDS/IPS foca na filtragem de tráfego com base em endereços IP e portas.
b) A função primária de um firewall é exercer controle de acesso à rede (permitir ou negar tráfego) com base em um conjunto de políticas predefinidas (regras). A função primária de um IDS/IPS é monitorar o tráfego de rede para identificar e responder a atividades maliciosas, comparando-as com assinaturas de ataques conhecidos ou detectando desvios de comportamento.
c) Um firewall opera exclusivamente nas camadas de rede e transporte (L3/L4), enquanto um IDS/IPS opera somente na camada de aplicação (L7), analisando o conteúdo específico dos protocolos.
d) A principal diferença é que o firewall sempre requer intervenção manual para bloquear uma ameaça, enquanto o IDS/IPS opera de forma totalmente autônoma.
e) Ambos os sistemas possuem a mesma função básica, sendo o IDS/IPS apenas uma evolução rebatizada do firewall tradicional.

QUESTÃO 32. O protocolo Secure Shell (SSH) é usado para acesso remoto seguro a servidores. Qual é a característica fundamental do SSH que está ausente no Telnet e que elimina o risco de espionagem (eavesdropping) da comunicação, incluindo as credenciais de login?

a) O SSH exige o uso de chaves públicas para autenticação, enquanto o Telnet não suporta esse método.
b) O SSH é compatível com mais sistemas operacionais do que o Telnet.
c) O SSH usa um firewall para proteger a comunicação, enquanto o Telnet não usa.
d) O SSH é mais rápido que o Telnet, pois usa um protocolo de compressão de dados.
e) O SSH usa criptografia para proteger a comunicação, enquanto o Telnet envia dados em texto puro.

QUESTÃO 33. Uma análise de risco é um processo crucial em segurança da informação. Qual é a principal diferença entre um risco e uma vulnerabilidade?

a) O risco é a probabilidade de um ataque ocorrer, e a vulnerabilidade é a ameaça de um ataque.
b) O risco é uma ameaça externa, e a vulnerabilidade é uma ameaça interna.
c) O risco e a vulnerabilidade são a mesma coisa, e os termos são usados de forma intercambiável.
d) O risco é o potencial de perda ou dano, e a vulnerabilidade é uma fraqueza em um sistema que pode ser explorada por uma ameaça.
e) O risco é o impacto de um ataque, e a vulnerabilidade é a fraqueza que pode ser explorada por um atacante.

QUESTÃO 34. Em um cenário de virtualização, um analista de segurança está revisando a segurança de um hypervisor tipo 1 (bare-metal). Qual é a principal característica de segurança de um hypervisor tipo 1, em comparação com um hypervisor tipo 2, e por que essa característica o torna mais seguro para cargas de trabalho críticas?

a) Um hypervisor tipo 1 é mais seguro, pois ele não precisa de uma conexão de rede, o que o torna imune a ataques de rede.
b) Um hypervisor tipo 1 é mais seguro, pois ele usa um firewall de aplicação para proteger as máquinas virtuais.
c) Um hypervisor tipo 1 é mais seguro, pois é executado diretamente sobre o hardware, dispensando um sistema operacional hospedeiro, o que reduz a superfície de ataque comparado ao tipo 2
d) Um hypervisor tipo 1 é mais seguro, pois ele tem um sistema operacional hospedeiro (host) que o protege de ataques.
e) Um hypervisor tipo 1 é mais seguro, pois ele usa criptografia para proteger as máquinas virtuais.

QUESTÃO 35. Em uma arquitetura de microsserviços, os serviços se comunicam por meio de APIs. Qual é o principal desafio de segurança ao implementar essa arquitetura, e qual é a melhor solução para mitigá-lo?

a) O principal desafio é o phishing, e a melhor solução é o treinamento de conscientização.
b) O principal desafio é o alto consumo de memória, e a melhor solução é usar um firewall de aplicação.
c) O principal desafio é a autenticação e a autorização dos serviços, pois cada serviço pode ter sua própria política de segurança. A melhor solução é usar um API Gateway para centralizar a autenticação e a autorização.
d) O principal desafio é a vulnerabilidade de buffer overflow, e a melhor solução é usar firewalls de aplicação.
e) O principal desafio é o man-in-the-middle, e a melhor solução é usar hashes para proteger a integridade dos dados.

QUESTÃO 36. Em um cenário de segurança de rede, um administrador de sistemas está revisando as regras de um firewall para proteger o servidor web da empresa. Ele precisa garantir que o tráfego do servidor web seja filtrado com base nas sessões. Qual é o tipo de firewall que ele deve usar e como ele funciona?

a) Um firewall de aplicação, que filtra o tráfego com base no conteúdo do pacote, como o protocolo HTTP.
b) Um firewall de rede, que filtra o tráfego com base nas informações do cabeçalho do pacote, como o endereço de IP e a porta.
c) Um firewall de pacote, que filtra o tráfego com base nas informações do cabeçalho do pacote, como o endereço de IP e a porta.
d) Um firewall de proxy, que atua como um intermediário entre o cliente e o servidor, e filtra o tráfego com base na sessão.
e) Um firewall de estado, que mantém o estado da conexão e filtra o tráfego com base na sessão, permitindo apenas o tráfego que pertence a uma conexão estabelecida.

QUESTÃO 37. A norma ISO/IEC 27001 define o SGSI (Sistema de Gestão de Segurança da Informação) e a norma ISO/IEC 27002 fornece um guia de implementação. Qual é a relação entre às duas?

a) A ISO 27001 se concentra em sistemas operacionais, enquanto a ISO 27002 se concentra em redes.
b) A ISO 27001 e a ISO 27002 são a mesma coisa, e ambos os termos são usados para descrever o processo de gestão de segurança.
c) A ISO 27001 define os requisitos para o SGSI, e a ISO 27002 fornece as diretrizes para a implementação dos controles de segurança.
d) Ambas as normas são obrigatórias para a certificação do SGSI.
e) A ISO 27001 é um guia para a implementação de controles de segurança, e a ISO 27002 define os requisitos para o SGSI

QUESTÃO 38. O SNMP (Simple Network Management Protocol) é amplamente utilizado para gerenciar dispositivos de rede. Embora o SNMPv2c tenha adicionado melhorias de desempenho, ele ainda utiliza community strings em texto claro, semelhante ao SNMPv1. Qual é o principal avanço de segurança introduzido pelo SNMPv3 em relação ao SNMPv2c, e como a escolha do nível de segurança authPriv aborda os três pilares da Segurança da Informação (CIA - Confidencialidade, Integridade e Disponibilidade)?

a) O principal avanço é a adição de traps de Camada 7; o authPriv garante a Disponibilidade (via traps) e a Integridade, mas a Confidencialidade deve ser implementada separadamente.
b) O principal avanço é o uso de community strings criptografadas; o authPriv protege a Integridade (com hashes) e a Disponibilidade, mas a Confidencialidade é garantida apenas pelo uso de TLS.
c) O principal avanço é a autenticação baseada em IPv6, e o authPriv garante a Confidencialidade e a Integridade, mas não a Disponibilidade.
d) O principal avanço é a introdução do Modelo de Segurança Baseado em Usuário (USM); o nível authPriv garante a Integridade (com algoritmos de hash como SHA ou MD5), a Confidencialidade (com algoritmos de criptografia como AES ou DES), mas não a Disponibilidade (que é uma preocupação de infraestrutura).
e) O principal avanço é o uso de OIDs criptografados; o 'authPriv' garante a Integridade (com a 'community string') e a Confidencialidade, mas deixa a Autenticação como responsabilidade do SO do dispositivo.

QUESTÃO 39. A vulnerabilidade Heartbleed (CVE-2014-0160) explorou uma falha de implementação do TLS/DTLS. Qual é a natureza exata dessa falha, e por que a exploração dela permitia que um atacante extraísse dados sensíveis, como chaves privadas de criptografia, da memória do servidor?

a) A falha era um erro de validação do padding na Cifra de Bloco do SSLv3, que permitia a descriptografia de dados por um ataque side-channel.
b) A falha era um erro de buffer overflow no código de criptografia, que permitia ao atacante injetar comandos assembly diretamente no kernel para desativar a criptografia TLS.
c) A falha era um erro de validação de entrada no campo length da requisição Heartbeat, que permitia a um cliente malicioso solicitar que o servidor retornasse mais dados do que o realmente contido no payload, expondo até 64 KB de memória arbitrária do servidor por requisição.
d) A falha explorava o uso de criptografia simétrica fraca (DES) no OpenSSL, permitindo um ataque de força bruta distribuída para quebrar a chave de sessão em menos de 24 horas.
e) A falha gera um erro de race condition durante o handshake do TLS, que permitia ao atacante se passar pelo servidor e receber as credenciais do usuário em texto claro antes da criptografia.

QUESTÃO 40. Em sistemas operacionais, um deadlock ocorre quando quatro condições estão presentes simultaneamente: Exclusão Mútua, Espera e Retenção (Hold and Wait), Não Preempção (No Preemption) e Espera Circular (Circular Wait).

Considere o seguinte cenário:

Dois processos, P1 e P2, precisam acessar dois recursos R1 e R2 para concluir uma tarefa.

P1 adquire R1 e solicita R2.

P2 adquire R2 e solicita R1.

Ambos os processos ficam bloqueados indefinidamente, aguardando o recurso mantido pelo outro.

Qual das quatro condições de deadlock é a que melhor descreve a relação de dependência direta entre P1 e P2 neste cenário?

a) Exclusão Mútua – porque cada recurso só pode ser usado por um processo por vez.
b) Espera e Retenção (Hold and Wait) – porque cada processo mantém um recurso enquanto espera por outro.
c) Não Preempção (No Preemption) – porque os recursos não podem ser retirados dos processos à força.
d) Espera Circular (Circular Wait) – porque P1 espera por R2 (segurado por P2) e P2 espera por R1 (segurado por P1), formando um ciclo de dependência.
e) Falta de Serialização – porque as operações não foram executadas em uma ordem sequencial.