FIOCRUZ

Concurso Público Fiocruz 2023

Tecnologista em Saúde Pública

Prova Objetiva e Discursiva

TE16

Tecnologia da informação e comunicação (TIC) com foco em segurança da informação

Prova Objetiva

01. Nos termos da Política Nacional de Segurança da Informação (PNSI), a competência para instituir o sistema de gestão de segurança da informação é do(a):

(A) Gestor(a) de Segurança da Informação.
(B) Alta Administração.
(C) Comitê Gestor de Segurança da Informação.
(D) Comitê Interno de Segurança da Informação.
(E) Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos.

02. Controles de segurança são políticas, métodos, técnicas ou procedimentos implementados para reduzir o risco de um agente de ameaça explorar uma vulnerabilidade. Os controles podem ser categorizados em físicos, lógicos e administrativos. Os seguintes controles lógicos são utilizados de forma predominantemente detectiva:

(A) access control lists (ACLs) e logs de auditoria.
(B) softwares de anti-malware e backup de dados.
(C) intrusion detection system (IDS) e criptografia.
(D) logs de auditoria e intrusion detection system (IDS).
(E) access control lists (ACLs) e backup de dados.

03. São serviços de segurança disponibilizados pela Amazon Web Services (AWS):

(A) Sentinel, CloudTrail e Cloud Armour.
(B) Cloud Armour, GuardDuty e Defender.
(C) Entra, Defender, Sentinel.
(D) Sentinel, Cognito e Cloud Armour.
(E) CloudTrail, GuardDuty e Cognito.

04. OpenID Connect é um(a):

(A) metodologia de provisionamento que eleva os usuários ao acesso privilegiado necessário para executar uma tarefa específica.
(B) camada de autenticação construída sobre o protocolo OAuth 2.
(C) padrão aberto para autorização de terceiros.
(D) serviço de segurança que autentica e autoriza usuários e é um mecanismo centralizado de controle de acesso.
(E) tecnologia que permite que um usuário se autentique uma vez e depois acesse recursos no ambiente sem precisar se autenticar novamente.

05. Suponha que você esteja desenvolvendo uma aplicação web que utiliza consultas SQL para interagir com um banco de dados. Considerando as boas práticas de prevenção de SQL injection preconizadas pela OWASP (Open Web Application Security Project), a abordagem para proteger o sistema contra esse tipo de ataque deve ser:

(A) utilizar consultas SQL dinâmicas com concatenação de strings.
(B) implementar uma blacklist de caracteres especiais e rejeitar qualquer entrada que contenha esses caracteres.
(C) validar e sanitizar todas as entradas de usuário antes de incorporá-las em consultas SQL.
(D) ocultar completamente mensagens de erro do banco de dados para evitar revelar informações sensíveis
(E) utilizar a função eval() para avaliar dinamicamente as consultas SQL com base nas entradas do usuário.

06. As seguintes ferramentas são utilizadas para port scan, EXCETO:

(A) nmap.
(B) nessus.
(C) metasploit.
(D) exploit-db.
(E) burp suite.

07. Spear phishing é um(a):

(A) tipo de ataque de phishing altamente direcionado.
(B) ato de falsificar a identidade da fonte de uma comunicação ou interação.
(C) forma de ataque de phishing que ocorre em VoIP.
(D) técnica maliciosa em que uma vítima é induzida a clicar em URL, botão ou outro objeto de tela que ela não tenha percebido e nem pretendido clicar.
(E) tipo específico de phishing que visa membros de alto escalação de organizações.

08. Malware é um software malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. O malware que tem como objetivo apagar e destruir os dados é conhecido como:

(A) ransomware.
(B) worm.
(C) trojan.
(D) rootkits.
(E) wiper.

09. A detecção e correção de incidentes de segurança da informação fazem parte da seguinte atividade da cadeia de valor do ITIL 4:

(A) melhoria.
(B) engajamento.
(C) desenho e transição.
(D) construção.
(E) entrega e suporte.

10. A Autoridade Nacional de Proteção de Dados (ANPD) poderá solicitar a agentes de tratamento a realização de estudos de impacto à proteção de dados pessoais, inclusive para avaliar os riscos à privacidade e à proteção dos dados. Com base na Lei Geral de Proteção de Dados Pessoais (LGPD), a afirmativa está:

(A) correta, pois a ANPD tem o poder de determinar a realização de estudos de impacto à proteção de dados pessoais, inclusive para avaliar os riscos à privacidade e à proteção dos dados.
(B) incorreta, pois a ANPD não tem o poder de determinar a realização de estudos de impacto à proteção de dados pessoais, mas apenas de recomendar sua realização.
(C) correta, mas apenas para os agentes de tratamento que operam com dados pessoais de crianças e adolescentes.
(D) incorreta, pois a ANPD só pode solicitar a realização de estudos de impacto à proteção de dados pessoais em casos de comprovado risco à privacidade e à proteção dos dado
(E) correta, mas apenas para os agentes de tratamento que operam com dados pessoais sensíveis.

11. O Open Worldwide Application Security Project (OWASP) é uma fundação sem fins lucrativos que trabalha para melhorar a segurança do software. Segundo a OWASP, em um processo de DevSecOps, o pipeline de DevSecOps deve seguir a seguinte sequência de execução de ferramentas:

(A) SCA, SAST, IAST e DAST.
(B) SAST, SCA, IAST e DAST.
(C) IAST, SAST, DAST e SCA.
(D) SCA, IAST, SAST e DAST.
(E) SAST, IAST, SCA e DAST.

12. Segundo o CIS Controls 8 – Cloud Companion Guide, a medida “13.2 Implantar uma solução de detecção de intrusão baseada em host” é aplicável ao(s) modelo(s) de nuvem:

(A) IaaS e PaaS.
(B) IaaS, apenas.
(C) IaaS, PaaS, SaaS e FaaS.
(D) FaaS, apenas.
(E) PaaS e SaaS.

13. Dentre os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD), há a realização do tratamento de dados pessoais para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Essa é a definição de:

(A) finalidade.
(B) adequação.
(C) qualidade de dados.
(D) necessidade.
(E) transparência.

14. A Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), derivada da Política Nacional de Segurança da Informação, determina que órgãos e entidades devem notificar o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), no caso de ocorrência de incidentes cibernéticos de maior impacto. Considerando o Programa de Privacidade e Segurança da Informação (PPSI), além do CTIR Gov, a Fiocruz deve notificar a ocorrência de incidentes cibernéticos ao(à):

(A) CERT.BR – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.
(B) CAIS/RNP – Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Ensino e Pesquisa.
(C) CISC Gov.br – Centro Integrado de Segurança Cibernética do Governo Digital.
(D) ANPD - Autoridade Nacional de Proteção de Dados Pessoais.
(E) Ministério da Saúde.

15. Conforme definido no Programa de Privacidade e Segurança da Informação (PPSI), a implementação do Framework de Privacidade e Segurança da Informação é de responsabilidade do(a):

(A) Gestor de Segurança da Informação.
(B) Encarregado pelo Tratamento de Dados Pessoais.
(C) Auditor-chefe.
(D) Estrutura de Governança.
(E) Gestor de Tecnologia da Informação.

16. A ITIL v4 propõe um modelo de gerenciamento de serviços de TI baseado em quatro dimensões. A alternativa que NÃO se configura como uma das quatro dimensões é:

(A) organizações e pessoas.
(B) informação e tecnologia.
(C) clientes e usuários.
(D) fluxos de valor e processos.
(E) parcerias e fornecedores.

17. De acordo com o CIS Controls 8, os seguintes controles NÃO possuem medidas de implementação obrigatória no âmbito de empresas de pequeno e médio porte:

(A) monitoramento e defesa da rede, segurança de aplicações e testes de invasão.
(B) inventário e controle de ativos corporativos, segurança de aplicações e gestão contínua de vulnerabilidades.
(C) monitoramento e defesa da rede, proteção de dados e testes de invasão.
(D) gestão e resposta a incidentes, gestão contínua de vulnerabilidades e recuperação de dados.
(E) testes de invasão, gestão de provedor de serviços e defesas contra malware.

18. Dentre as hipóteses de não aplicabilidade da Lei Geral de Proteção de Dados Pessoais (LGPD), está o tratamento de dados pessoais realizado:

(A) por pessoa natural para fins exclusivamente particulares e econômicos.
(B) exclusivamente para políticas de saúde pública.
(C) para fins exclusivos de segurança de Estado.
(D) exclusivamente para implementação de políticas públicas.
(E) após o consentimento do titular de dados pessoais.

19. O STRIDE é um framework de modelagem de ameaças utilizado em ambientes de DevSecOps. Dentre as categorias de ameaças do STRIDE, o DOS e o Spoofing afetam, respectivamente, as seguintes propriedades de segurança:

(A) autenticação e disponibilidade.
(B) autorização e autenticação.
(C) disponibilidade e confidencialidade.
(D) não-repúdio e confidencialidade.
(E) disponibilidade e autenticação.

20. O Microsoft Azure Bastion é uma solução de segurança em nuvem utilizada para:

(A) conectividade com o ambiente Azure.
(B) privacidade.
(C) conformidade.
(D) gerenciamento de eventos.
(E) gestão de identidades.

21. Dos mecanismos, tecnologias e controles de segurança da informação apresentados abaixo, aquele que é utilizado para garantir que apenas usuários autorizados tenham acesso a recursos de rede e sistemas de informação é:

(A) firewall.
(B) sistema de detecção de intrusão (IDS).
(C) rede virtual privada (VPN).
(D) controle de acesso.
(E) antivírus.

22. Dentre os métodos de autenticação apresentados, aquele que é considerado o mais seguro para identificar um usuário antes de acessar um recurso computacional ou sistema de informação é:

(A) senha de uso único (OTP) enviada por e-mail.
(B) certificado digital para identificação de pessoa física.
(C) biometria.
(D) autenticação em dois fatores (2FA) utilizando senha e confirmação enviada por SMS.
(E) token de hardware.

23. Sobre criptografia de dados, avalie se as afirmativas a seguir são verdadeiras (V) ou falsas (F):

I - O algoritmo RSA é amplamente utilizado para criptografia simétrica, garantindo a segurança dos dados em trânsito.
II - O uso de chaves públicas na criptografia assimétrica permite que qualquer pessoa possa criptografar uma mensagem, mas apenas o destinatário com a chave privada correspondente pode descriptografá-la.
III - A criptografia assimétrica é mais rápida que a criptografia simétrica, tornando-a ideal para criptografar grandes volumes de dados antes de realizar sua transmissão.

As afirmativas I, II e III apresentadas são respectivamente:

(A) V, V e F.
(B) V, F e V.
(C) F, V e V.
(D) V, F e F.
(E) F, V e F.

24. A alternativa correta a respeito dos componentes e do funcionamento dos processadores e da arquitetura dos computadores é a seguinte:

(A) memória cache L3 é maior e mais rápida do que memória cache L1.
(B) processadores com arquitetura Reduced Instruction Set Computer (RISC) tendem a ter um conjunto menor de instruções, o que resulta em instruções mais complexas.
(C) a unidade de controle é o componente responsável por executar operações aritméticas e lógicas do processador.
(D) a tecnologia Hyper-Threading duplica fisicamente os núcleos de um processador, o que causa um aumento do seu desempenho geral.
(E) a tecnologia Direct Memory Access (DMA) permite que a controladora de um dispositivo de entrada e saída acesse diretamente a memória principal, reduzindo a dependência do processador e tornando o sistema mais rápido.

25. Sobre a memória RAM dos computadores, a única opção correta dentre as alternativas abaixo é:

(A) a memória DDR5 consome menos energia do que as memórias nos padrões DDR4, DDR3 e DDR2, embora seja também mais rápida do que as demais.
(B) todos os arquivos e programas instalados e copiados para o computador são permanentemente armazenados na memória RAM, o que permite que sejam usados depois que ele é desligado e ligado novamente.
(C) a memória SRAM é um tipo de RAM que precisa ser constantemente atualizada para que não ocorra perda gradual dos dados armazenados.
(D) SDRAM é um tipo de memória que funciona de forma independente e assíncrona com relação ao clock do computador.
(E) memórias DRAM são mais rápidas do que SRAM porque precisam que as informações armazenadas nelas sejam constantemente atualizadas.

26. Leia as afirmativas a seguir sobre processadores e sistemas multiprocessados.

I – Os processadores têm registradores que são visíveis ao usuário, que podem ser referenciados em código e servem para guardar endereços, dados e flags, e registradores de controle de estado, que têm funções específicas, como armazenar instruções, endereços de instruções que serão lidas e servir de buffer de dados.
II – A técnica de pipeline permite que processadores realizem diferentes instruções ao mesmo tempo, de forma que uma instrução que está em um estágio de execução possa ser processada ao mesmo tempo que outra instrução que está em outro estágio.
III – A técnica de divisão de um processo em múltiplos threads que podem ser executados ao mesmo tempo pelo processador é também conhecida como multiprocessamento assimétrico.

Das afirmativas acima:

(A) somente I e II estão corretas.
(B) somente I e III estão corretas.
(C) somente II e III estão corretas.
(D) somente II está correta.
(E) somente III está correta.

27. Sobre segurança em sistemas de arquivos, as listas de controle de acesso (ACL):

(A) só podem ser utilizadas em sistemas de arquivos FAT nativo de sistemas operacionais UNIX e Linux.
(B) consistem em listas contendo usuários e grupos e suas respectivas permissões de acesso a arquivos ou diretórios aos quais estão associadas e podem ser utilizados em sistemas operacionais Linux, UNIX e Windows.
(C) estão disponíveis somente em sistemas operacionais Windows e somente para sistemas de arquivos NTFS, ext3 e ext4.
(D) podem ser implementadas apenas em sistemas operacionais que executam algum serviço de firewall e que estejam ligados a uma rede de computadores.
(E) podem permitir ou restringir o acesso de grupos de usuários a arquivos e diretórios em sistemas operacionais Windows, Linux e UNIX, mas não podem definir permissões a usuários individuais.

28. A arquitetura de protocolos TCP/IP:

(A) utiliza na camada de rede o Internet Protocol (IP), que é confiável e garante a entrega dos dados no host de destino.
(B) especifica o Internet Control Message Protocol (ICMP) como protocolo de transmissão de mensagens de correio eletrônico entre um host de origem e um host de destino.
(C) determina que Point-to-Point Protocol (PPP) e Carrier Sense Multiple Access with Collision Detection (CSMA/CD) são os padrões de camada de Enlace de Dados.
(D) especifica os protocolos User Datagram Protocol (UDP) e Stream Control Transmission Protocol (SCTP) como protocolos da camada de Transporte.
(E) utiliza na camada de Aplicação o Address Resolution Protocol (ARP), que possibilita a resolução de nomes em endereços IP a fim de facilitar a identificação de hosts pelos seres humanos.

29. A filial de uma organização recebeu da sede para utilizar em sua rede local o bloco de endereços IPv4 17.12.40.0/26. O administrador da rede precisa dividir esse bloco de endereços em três sub-redes separadas por roteador de maneira que os 8 servidores fiquem em uma sub-rede isolada dos demais computadores, e que os 20 computadores do departamento de produção fiquem em uma sub-rede diferente dos 10 computadores do departamento de administração.

Com base na situação descrita acima, avalie se são corretas ou incorretas cada uma das afirmativas apresentadas a seguir:

I – A máscara de sub-rede do bloco de endereços 17.12.40.0/26 disponibilizado pela sede da organização para a filial é 255.255.255.192, é o que permite à filial ter 64 endereços disponíveis para utilizar em suas sub-redes.
II – É possível dividir o bloco de endereços 17.12.40.0/26 em duas sub-redes diferentes mudando o CIDR para /25, o que permite dividir o bloco designado pela sede da organização em dois blocos de 32 endereços.
III – A filial poderá utilizar a máscara de sub-rede 255.255.255.224 e a faixa de endereços IP que vai de 17.12.40.0 a 17.12.40.31 na sub-rede do departamento de produção, a máscara de sub-rede 255.255.255.240 e a faixa de endereços IP que vai de 17.12.40.32 a 17.12.40.47 para a sub-rede dos servidores, e a máscara de sub-rede 255.255.255.240 e a faixa de endereços IP que vai de 17.12.40.48 a 17.12.40.63 para a sub-rede do departamento de administração.

Das afirmativas acima:

(A) apenas I e II estão corretas.
(B) apenas II e III estão corretas.
(C) apenas I e III estão corretas.
(D) apenas III está correta.
(E) todas estão corretas.

30. O modo passivo do protocolo FTP:

(A) deixa o cliente responsável por estabelecer a conexão para envio de comandos com a porta TCP 21 do servidor e por estabelecer a conexão para troca de dados com a porta TCP informada pelo servidor FTP.
(B) permite que o cliente estabeleça a conexão para envio de comandos com a porta TCP 21 do servidor, enquanto o servidor FTP utiliza a porta TCP 20 para estabelecer a conexão para troca de dados com a porta TCP informada pelo cliente.
(C) permite que a troca de comandos e dados entre o cliente e o servidor FTP ocorra utilizando somente a porta TCP 21 do servidor, não sendo necessária uma outra conexão entre cliente e servidor utilizando outra porta.
(D) deixa o cliente responsável por estabelecer a conexão para envio de comandos com a porta TCP 21 e outra conexão para troca de dados com a porta TCP 20 do servidor.
(E) permite que a troca de comandos e dados entre o cliente e o servidor FTP ocorra utilizando somente a porta TCP 20 do servidor, não sendo necessária uma outra conexão entre cliente e servidor utilizando outra porta.

31. Analise o fragmento do arquivo de log apresentado abaixo:

Feb 11 10:15:22 firewall kernel: [1234567.123456] Dropped 100 SYN packets from 192.168.1.110:1234 to 203.0.113.5:80, rate-limit exceeded
Feb 11 10:15:25 firewall kernel: [1234567.123457] Dropped 150 SYN packets from 192.168.1.101:5678 to 203.0.113.5:80, rate-limit exceeded
Feb 11 10:15:28 firewall kernel: [1234567.123458] Dropped 120 SYN packets from 192.168.1.122:9876 to 203.0.113.5:80, rate-limit exceeded

Aparentemente, esse fragmento de log de firewall mostra:

(A) três tentativas bem-sucedidas de acesso ao endereço 203.0.113.5 na porta TCP 80 a partir dos endereços 192.168.1.101, 192.168.1.110 e 192.168.1.122.
(B) três tentativas malsucedidas de acesso a partir do endereço 203.0.113.5 aos endereços 192.168.1.110, 192.168.1.101 e 192.168.1.122 nas portas TCP 1234, 5678 e 9876, respectivamente.
(C) três tentativas malsucedidas de ataque de negação de serviço SYN Flood com origem nos endereços 192.168.1.110, 192.168.1.101 e 192.168.1.122 contra o endereço 203.0.113.5 na porta TCP 80.
(D) três tentativas bem-sucedidas de ataque de negação de serviço SYN Flood a partir do endereço 203.0.113.5 contra os endereços 192.168.1.110, 192.168.1.101 e 192.168.1.122 nas portas TCP 1234, 5678 e 9876, respectivamente.
(E) três tentativas malsucedidas de acesso ao endereço 203.0.113.5 nas portas TCP 1234, 5678 e 9876 a partir dos endereços 192.168.1.110, 192.168.1.101 e 192.168.1.122.

32. Sistemas de detecção de intrusão (IDS) são:

(A) melhores do que sistemas de prevenção de intrusão (IPS) por informarem ao administrador de segurança da informação quando há comportamento típico de ataque identificado na rede, o que o IPS não faz.
(B) exclusivamente baseados em host, ou seja, precisam ser instalados e configurados em servidores e clientes da rede para funcionarem, enquanto sistemas de prevenção de intrusão (IPS) podem ser baseados em rede ou em host, a depender do tipo implantado na rede.
(C) responsáveis por configurar automaticamente recursos de segurança nos firewalls, servidores e clientes da rede quando há comportamentos típicos de ataques identificados.
(D) passivos, pois não alteram configurações de firewalls, servidores e clientes em decorrência de comportamentos de intrusão detectados na rede, enquanto sistemas de prevenção de intrusão (IPS) têm um comportamento ativo, podendo registrar e bloquear o comportamento de intrusão.
(E) pouco eficientes, pois podem detectar um falso positivo e, como consequência, podem configurar firewalls, servidores e clientes da rede e prejudicar seu funcionamento.

33. Em uma grande organização, com diversas filiais e escritórios descentralizados, o departamento de Tecnologia da Informação está implantando uma solução de rede virtual privada (VPN) para conectar filiais e equipes localizados em diferentes cidades. A equipe técnica está considerando tanto redes client-to-site quanto redes site-to-site para atender às necessidades de comunicação dos usuários.

Analise as seguintes afirmativas, avaliando se são verdadeiras ou falsas:

I – Os usuários remotos que trabalham em filiais conectadas com a sede através de VPN site-to-site necessitam de um cliente VPN instalado em seus computadores para acessarem a rede da sede da organização quando estiverem trabalhando nas redes de computadores das suas filiais.
II – Filiais podem se conectar à sede da organização utilizando VPN site-to-site, criando uma extensão virtual da rede corporativa utilizando a Internet pública para trafegar dados de forma segura.
III – Tanto redes client-to-site quanto redes site-to-site oferecem segurança para trafegar dados pela Internet pública, pois é utilizada criptografia para proteger os dados que trafegam em ambos os tipos de VPN.

Das afirmativas acima:

(A) somente I e II são verdadeiras.
(B) somente II é verdadeira.
(C) todas as afirmativas são verdadeiras.
(D) somente I e III são verdadeiras.
(E) somente II e III são verdadeiras.

34. Para garantir a segurança em uma rede sem fio:

(A) o campo Wired Equivalent Privacy (WEP) de um frame no padrão 802.11 utiliza RC4 de 256 bits para criptografar cabeçalho e campo de dados, garantindo confidencialidade, integridade e autenticação na comunicação entre o cliente de rede sem fio e o Access Point (AP).
(B) é possível utilizar controladores de rede sem fio, que são servidores com capacidade de gerenciar a autenticação e segurança dos clientes da rede, mas não são capazes de interferir no funcionamento dos Access Points (AP) utilizados na infraestrutura da rede sem fio.
(C) o Wi-Fi Protected Access 2 (WPA2) substitui o Wired Equivalent Privacy (WEP) e Wi-Fi Protected Access (WPA), utilizando criptografia AES de 128 bits e suportando autenticação Remote Authentication Dial In User Service (RADIUS).
(D) o Wi-Fi Protected Access (WPA) é um protocolo que implementa Temporal Key Integrity Protocol (TKIP) para utilizar uma mesma chave de 128 bits para todos os frames trocados entre o cliente e o Access Point (AP).
(E) é possível ocultar o Service Set Identifier (SSID) do Beacon Frame enviado por um Access Point (AP), o que é suficiente para garantir sua segurança, pois não há como um cliente estabeleça conexão com o AP sem saber o seu SSID.

35. Soluções e técnicas de Controle de Acesso à Rede (NAC):

(A) tem como uma das suas principais funções determinar quais dispositivos podem estabelecer uma conexão com a rede de computadores e o que esses dispositivos podem acessar através de uma política de segurança predeterminada.
(B) permitem monitorar o acesso de dispositivos da organização e de seus funcionários à rede corporativa de computadores, mas não oferecem qualquer tipo de controle sobre dispositivos particulares de visitantes e fornecedores.
(C) envolvem um processo com autenticação e autorização de acesso de clientes à rede, mas não fazem nenhum tipo de gerenciamento visando ao cumprimento de política de segurança nem aplicação de planos de resposta a incidentes.
(D) são eficientes no controle de acesso de pré-admissão, pois avaliam o dispositivo antes de conceder acesso, mas não impedem que dispositivos autenticados e autorizados acessem diferentes recursos da rede de computadores lateralmente.
(E) necessitam de agentes para controlar o acesso de diferentes dispositivos à rede de computadores da organização.

36. Soluções de Controle de Acesso à Rede (NAC) avançadas contam com os seguintes recursos e funcionalidades, EXCETO:

(A) definição de políticas de acesso à rede local corporativa.
(B) autenticação de dispositivos corporativos que estiverem distantes da rede local corporativa.
(C) autenticação de dispositivos corporativos para acesso à rede local corporativa.
(D) visibilidade dos dispositivos corporativos com acesso à rede local corporativa.
(E) autorização de usuários credenciados para acesso à rede local corporativa.

37. Sobre o sistema operacional Linux, é correto afirmar que:

(A) embora existam diferentes versões do sistema operacional, as funcionalidades existentes, as interfaces e os pacotes disponíveis para instalação em diferentes sistemas Linux são os mesmos, pois todos utilizam o mesmo kernel.
(B) a forma como as permissões de contas de usuário e grupos a arquivos e diretórios são concedidas é diferente de como é feito em computadores com sistema operacional UNIX.
(C) ele não dispõe de recursos de auditoria e registro de eventos que permitam monitorar atividades executadas no sistema.
(D) é possível integrar um computador com esse sistema operacional a um Active Directory como cliente ou servidor de arquivos com a instalação e configuração do pacote SAMBA.
(E) não há um firewall nativo desse sistema operacional que possa ser utilizado para configurar listas de controle de acesso para impedir ou permitir o acesso ao computador pela rede de computadores.

38. Dentre as alternativas abaixo, a única que apresenta características típicas de um Firewall UTM é:

(A) backup de dados armazenados em servidores da rede, filtro de pacotes e filtro de conteúdo.
(B) IPS, antivírus, instalação de atualizações em sistemas operacionais de clientes e servidores.
(C) inspeção profunda de pacotes, gerenciamento centralizado de contas de usuário e filtro de pacotes stateful.
(D) IDS, gerenciamento de senhas de usuários do Active Directory e VPN.
(E) autorização de acesso de usuários e dispositivos, antispam e registro de eventos em log.

39. Ao comparar os sistemas operacionais Windows e Linux, é possível afirmar que:

(A) o Linux pode substituir totalmente o Windows em um domínio Active Directory, bastando para isto instalar e configurar os pacotes gratuitos ADLinux, SAMBA e BIND no servidor Linux, de forma que ele passe a funcionar como controlador de domínio, servidor DNS e servidor de arquivos.
(B) a comunidade de profissionais que trabalham com Linux revisa extensivamente seu código, facilitando a identificação e correção de falhas de segurança, enquanto a fabricante do Windows disponibiliza atualizações e correções de vulnerabilidades.
(C) o Linux permite que sejam definidas quotas de uso do disco para usuários a fim de limitar o uso de disco, enquanto o Windows não oferece essa possibilidade.
(D) o sistema de arquivos ext4 suporta journaling como forma de garantir a integridade do disco em caso de falhas, enquanto o sistema de arquivos NTFS não dispõe desse recurso.
(E) enquanto servidores Linux podem ser acessados remotamente pelos administradores por meio de terminais utilizando SSH ou Telnet, servidores Windows não podem ser acessados remotamente por terminal, o que impede sua administração remota.

40. São alternativas para prevenir a quebra de autenticação e a quebra de controle de acesso em um sistema:

(A) exigir a utilização de senhas longas e complexas e desconsiderar os perfis de usuários ao definir permissões de acesso.
(B) utilizar as mesmas credenciais padrão para todos os usuários e registrar em log e notificar falhas de controle de acesso.
(C) utilizar a autenticação multifator e bloquear sessão após um período de inatividade.
(D) permitir a repetição de senhas utilizadas anteriormente e utilizar o princípio de menor privilégio para conceder acesso.
(E) limitar a quantidade de tentativas de autenticação com falha e manter as permissões de acesso de colaboradores desligados da organização.

Prova Discursiva

QUESTÃO

Você foi contratado como consultor de segurança da informação por uma organização que planeja implementar um novo firewall UTM em sua rede. Explique como você recomendaria a configuração e o uso do firewall UTM tendo em vista a segurança da rede organizacional abordando os seguintes aspectos:

a) Controle de acesso de usuários e dispositivos a recursos da rede local e da Internet.
b) Autenticação de usuários para acesso a recursos da rede local e da Internet.
c) Criação de Zona Desmilitarizada (DMZ).
d) Integração com antivírus em clientes e servidores.
e) Integração com anti-spam em servidores de correio eletrônico.
f) Detecção e registro em log de eventos ocorridos em firewall, rede, clientes e servidores.
g) Prevenção de incidentes de segurança.
h) Geração e emissão de relatórios.

Escreva um texto com no mínimo 50 linhas e no máximo 150 linhas em resposta ao caso apresentado.

RASCUNHO

RASCUNHO

RASCUNHO

RASCUNHO

RASCUNHO

INSTRUÇÕES

1. Por motivo de segurança, a Fiocruz solicita que o candidato transcreva em letra cursiva, em espaço próprio no Cartão de Respostas da Prova Objetiva, a frase abaixo apresentada:

"As melhores coisas da vida não podem ser vistas nem tocadas, mas sim sentidas pelo coração." (Dalai Lama)

2. Para cada uma das questões da prova objetiva são apresentadas 5 (cinco) alternativas classificadas com as letras (A), (B), (C), (D) e (E), e só uma responde da melhor forma possível ao quesito proposto. Você só deve assinalar UMA RESPOSTA. A marcação de nenhuma ou de mais de uma alternativa anula a questão, MESMO QUE UMA DAS RESPOSTAS SEJA A CORRETA.
3. A duração da prova é de 4 (quatro) horas, considerando, inclusive, a marcação do Cartão de Respostas e a Prova Discursiva. Faça-a com tranquilidade, mas controle o seu tempo.
4. Verifique se a prova é para o **PERFIL** para o qual concorre.
5. Somente após autorizado o início da prova, verifique se este Caderno de Questões está completo e em ordem. Folhear o Caderno de Questões antes do início da prova implica na eliminação do candidato.
6. Verifique, no **Cartão de Respostas da Prova Objetiva**, se seu nome, número de inscrição, identidade e data de nascimento estão corretos. Caso contrário, comunique ao fiscal de sala.
7. O **Caderno de Questões** poderá ser utilizado para anotações, mas somente as respostas assinaladas no **Cartão de Respostas da Prova Objetiva** e no **Caderno de Respostas da Prova Discursiva** serão objeto de correção.
8. Observe as seguintes recomendações relativas ao **Cartão de Respostas da Prova Objetiva**:
. não haverá substituição por erro do candidato;
. não deixar de assinar no campo próprio;
. não pode ser dobrado, amassado, rasurado, manchado ou conter qualquer registro fora dos locais destinados às respostas;
. a maneira correta de marcação das respostas é cobrir, fortemente, com esferográfica de tinta azul ou preta, o espaço correspondente à letra a ser assinalada;
. outras formas de marcação diferentes da que foi determinada acima implicarão a rejeição do **Cartão de Respostas**;
9. O fiscal não está autorizado a alterar quaisquer dessas instruções.
10. Você só poderá retirar-se da sala após 60 minutos do início da prova.
11. Quaisquer anotações só serão permitidas se feitas no caderno de questões.
12. Você poderá anotar suas respostas da prova objetiva em área específica do Caderno de Questões, destacá-la e levar consigo.
13. Os três últimos candidatos deverão permanecer na sala até que o último candidato entregue ao fiscal todo o seu material de prova.
14. Ao terminar a prova, entregue ao fiscal de sala, obrigatoriamente, o **Cartão de Respostas da Prova Objetiva, o Caderno de Respostas da Prova Discursiva e o Caderno de Questões**.

15. Prova Discursiva:

- A questão discursiva deverá ter um limite mínimo de 50 linhas e máximo de 150 linhas.

- Transcreva sua resposta para a parte pautada do **Caderno de Respostas da Prova Discursiva**. Não assine, rubrique ou coloque qualquer marca que o identifique, sob pena de ser anulado. Assim, a detecção de qualquer marca identificadora no espaço destinado à transcrição do texto definitivo acarretará nota ZERO na respectiva prova discursiva.

- O tempo total de duração das provas será de 4 (quatro) horas, incluindo o tempo para o preenchimento da Resposta Definitiva da Questão Discursiva. Nenhum rascunho SERÁ LEVADO EM CONTA.

Boa Prova!

Ao término da prova, anote aqui suas respostas e destaque na linha pontilhada.

01	09	17	25	33
02	10	18	26	34
03	11	19	27	35
04	12	20	28	36
05	13	21	29	37
06	14	22	30	38
07	15	23	31	39
08	16	24	32	40