Correção da Prova - A

Ary Felipe Farah e Silva

1. ***NOME***
2. ***EMAIL***
3. **Relacione as características fundamentais da informação que a Segurança da Informação visa prover, e explique-as**

   A Segurança da Informação conta com 3 pilares: Confidencialidade, Integridade e Disponibilidade.

   Confidencialidade - garante o acesso à informação somente por usuários autorizados.

   Integridade - garante que a mensagem permaneça igual, sem perdas ou mudanças indesejadas. Suas alterações devem ser autorizadas e documentadas.

   Disponibilidade - Garante que a informação seja acessível para aqueles que a buscam, de forma coerente com sua necessidade.

4. **Por que é importante documentar circunstâncias excepcionais que exijam o uso de identificadores de usuário compartilhados?**

   Essa é uma diretriz presente na norma **ISO 27002**, que orienta no processo de identificação e autenticação do usuário. Ela é importante para monitorar quem mexeu no dispositivo em cada momento, o que fez e por que. Assim é possível responsabilizar os indivíduos caso algo aconteça.

5. **Na atividade prática da Aula 4 - Autenticação, foi usada a autenticação multifator para o envio de e-mails por meio da plataforma do Google, o**

gmail. Quais são as opções oferecidas pela plataforma para a verificação em duas etapas?

As opções oferecidas pela plataforma são: **Mensagem de Texto** e **Chamada Telefônica**.

6. **Relacione e descreva os modelos de controle de acesso apresentados no conteúdo da disciplina.**

   Os modelos mais tradicionais de Controle de Acesso são:

   DAC - Discretionary Access Control: Esse controle é baseado na identidade do solicitante, definindo o que o indivíduo está autorizado a fazer. Esse indivíduo pode conceder acesso a outros sobre seus recursos.

   MAC - Mandatory Access Control: Esse controle é baseado na comparação de rótulos com autorizações de seguraça. enquanto o primeiro define a criticidade dos recursos do sistema, o segundo define quais indivíduos têm permissão de acesso a esses recursos. O indivíduo não pode conceder acesso a outros sobre seus recursos.

   RBAC - Role Based Access Control: Esse controle é baseado nos papéis de um indivíduo, definido regras de quais acessos cabem a diferentes papéis.

7. **O que é recomendado ao incluir-se um usuário na lista daqueles que podem utilizar a escalação de privilégio com o comando "sudo"?**

   É recomendado utilizar o comando `visudo` , que faz uma cópia temporária do arquivo sudoers, verificando erros de configuração e sintaxe.

8. ***FEEDBACK***
9. ***FEEDBACK***
10. ***FEEDBACK***

11. **Qual é o princípio de segurança que preconiza a restrição de privilégios de acesso apenas ao necessário para a realização das atividades?**

Princípio do Menor Privilégio. Esse é o conceito que diz que um usuário deve ter acessso apenas ao que é estritamente necessário para desempenhar suas funções.

12. **A autenticação multifator é uma técnica importante para garantir a segurança dos sistemas de informação. Considerando os fatores básicos de autenticação, qual dos seguintes exemplos se enquadra em "algo que o indivíduo possui"?**

    Senha descartável é algo que o indivíduo possui, pois dentro das 4 classificações (o que sabe, características físicas ou comportamentais) é o que mais se encaixa. Não é nenhuma característica e não é algo que o indivíduo sabe, já que é utilizada uma vez e descartada, sem objetivo de decorá-la.

13. **Na atividade sobre Controle de Acesso no LINUX foram abordadas as permissões especiais, que alteram o comportamento padrão do sistema operacional no trato de arquivos e diretórios. Entre estas, a que não tem efeito sobre diretórios é:**

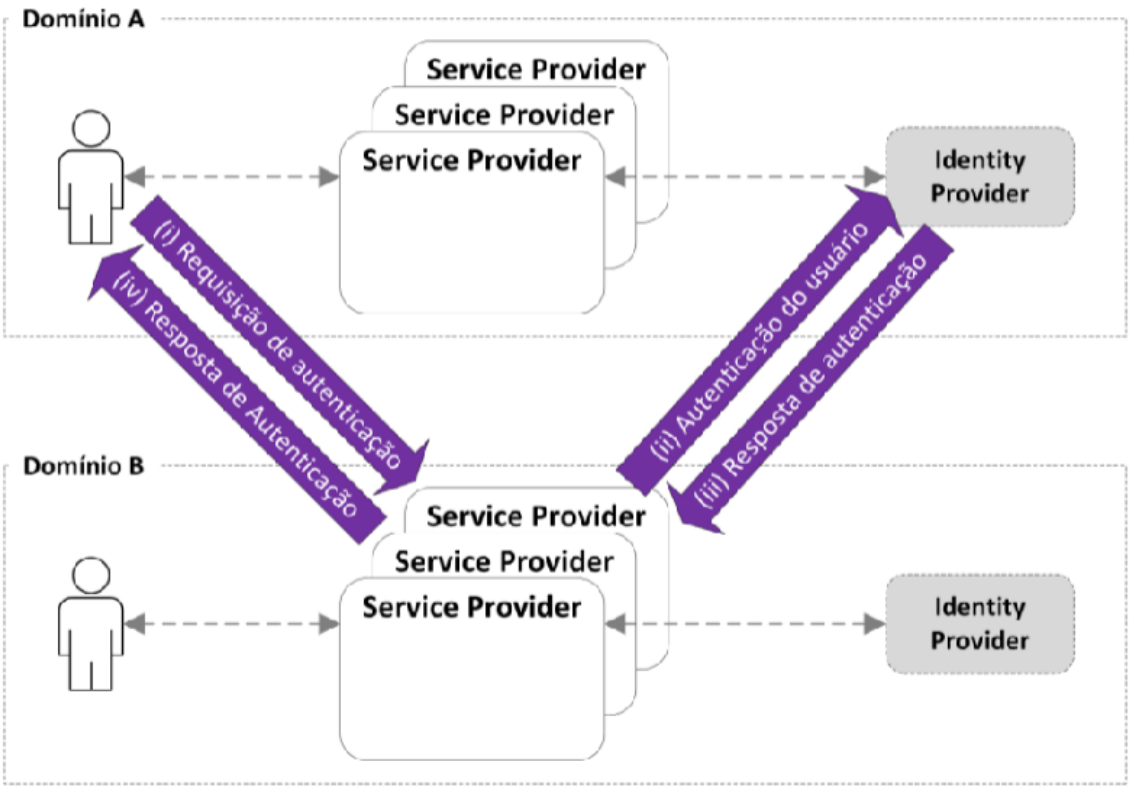
    A permissão SUID não tem efeito sobre diretórios, somente em arquivos executáveis.

14. **O Controle de Acesso é um mecanismo essencial para limitar ações e operações que determinados sujeitos podem realizar sobre um recurso, contribuindo para a segurança da informação. Considerando esse contexto, qual dos itens listados a seguir que estabelece que os usuários devem ter apenas os acessos necessários para realizar suas funções?**

    O Princípio do Menor Privilégio estabele que usuários devem ter acesso somente ao que é estritamente necessário para realizar suas funções.

15. **Os modelos de IdM (Identity Manager) desempenham um papel fundamental na gestão de identidades e acessos em sistemas de informação. Qual dos seguintes modelos de IdM envolve a colaboração entre diferentes organizações para facilitar o acesso aos serviços?**

O Modelo Federado utiliza da colaboração entre diferentes empresas, facilitando o acesso aos serviços.



16. **A autenticação de mensagens é um mecanismo importante na segurança da informação. O Message Authentication Code (MAC) é uma técnica que utiliza uma chave secreta compartilhada para gerar um código de autenticação que pode ser verificado pelo destinatário. Qual é o objetivo principal da autenticação de mensagens?**

    A autenticação de mensagens serve principalmente para verificar a integridade e autenticidade delas, já que esses atributos garantem a origem legitma da mensagem e se ela foi alterada ou não durante a transação.

17. **Com relação às tecnicas criptográficas estudadas, é correto afirmar que:**

    O HASH é uma técnica criptográfica irreversível, dado que não é possível descobrir o texto às claras (mensagem original) através de seu hash.

18. ***FEEDBACK***

19. ***FEEDBACK***

20. **A norma ISO 27002 fornece diretrizes importantes para o processo de identificação e autenticação de usuários em ambientes corporativos. De acordo com a norma, qual das seguintes práticas é recomendada para garantir a segurança da autenticação?**
    A prática mais correta é: “Implementar controles adicionais quando identificadores de usuário compartilhado são necessários”, já que as outras 3 contradizem escritas da norma

    “Documentar circunstâncias excepcionais que exijam utilização de identificador de usuário compartilhado por um grupo de pessoas.”

21. **A gestão de identidades é essencial para garantir a segurança e eficiência no acesso a sistemas e recursos computacionais. Considerando a importância da autenticação única - SSO (Single Sign On), qual é o principal benefício dessa abordagem?**

    O principal benefício dessa abordagem é a redução da complexidade de gerenciamento de senhas, já qie o indivíduo não precisa memorizar muitas senhas diferentes.

22. **Qual é a principal diferença entre Esteganografia e Esteganálise?**
    Esteganografia: técnica de ocultar mensagens
    Esteganálise: detecção e extração dessas mensagens.

23. **A autenticação é um processo fundamental para garantir a segurança da informação em ambientes digitais. Diversos métodos e tecnologias são utilizados para verificar a identidade dos usuários. Considerando a importância da autenticação, qual das seguintes afirmações está correta?**

    O método mais seguro é a autenticação biométrica, já utiliza características únicas de um indivíduo para verificar sua identidade.