**UC Sistemas Computacionais e Segurança – 2025.1**

**Exercícios de Revisão**

**Prof. Calvetti**

# Fontes de estudo principais

* Material curado da UC Sistemas Computacionais e Segurança no U-Life
* Curso Cisco Fundamentos de Segurança Cibernética
* Material das aulas

# Questões

1. O que é um *pentest*? Quais são as etapas de um *pentest*?

O Pentest vem do inglês penetration test, que significa teste de penetração. Esse teste é capaz de medir as vulnerabilidades em sistemas através de um conjunto de testes, invasões que simulam um ataque cracker.

1. Explique o funcionamento de 3 ataques de segurança cibernética que podem comprometer diretamente a DISPONIBILIDADE de sistemas.

Os ataques de negação de serviço são projetados para interromper a disponibilidade de um serviço, por exemplo:

Ataques DoS Distribuídos (DDoS): Em um Ataque DDoS, várias máquinas (geralmente computadores infectados ou recursos baseados em nuvem) enviam muitas solicitações de spam para um serviço. Como um aplicativo, o sistema que o hospeda e suas conexões de rede possuem larguras de banda finitas, o invasor pode exceder esses limites e tornar o serviço indisponível para usuários legítimos.

Ataques Ransom DoS (RDoS): Em um Ataque RDoS, o invasor exige um resgate para não realizar um ataque DDoS contra uma organização ou para interromper um ataque DDoS em andamento. Esses ataques podem ser campanhas autônomas ou combinados com um ataque de ransomware para fornecer ao invasor uma vantagem adicional para forçar a vítima a pagar o resgate.

Exploração de vulnerabilidade: O aplicativo pode ter erros lógicos, como uma vulnerabilidade de buffer overflow, que pode causar falha se for explorado. Se um invasor explorar essa vulnerabilidade, poderá realizar um ataque DoS contra o serviço vulnerável.

1. Leia o fragmento de texto a seguir.

Todas as empresas devem observar a legislação local, os seus regulamentos internos e as obrigações contratuais, além dos acordos internacionais. Os requisitos de segurança que uma empresa deve cumprir estão fortemente relacionados a isso. (HINTZBERGEN, 2018)

O texto acima se refere a um conceito que pode ser considerado importante quando se trata de segurança da informação. De qual conceito estamos falando (em uma palavra)?

Conformidade.

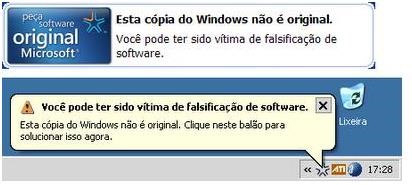
1. Existem vários recursos de software e hardware para estabelecer diversos níveis de segurança em uma rede de computadores. Entre outros, podemos citar os *firewalls* e os sensores (IDS e IPS). Faça um quadro comparativo resumindo as características de cada um dos três recursos.

|  |  |  |  |
| --- | --- | --- | --- |
|  | FireWall | IDS | IPS |
| Função | Controlar o tráfego de entrada e saída com base em regras | |  | | --- | |  |  |  | | --- | | Monitorar e identificar atividades suspeitas | | Monitorar, identificar e bloquear ameaças em tempo real |
| Ação | **Permite ou bloqueia** tráfego | Detecta e alerta | Detecta e impede |
| Posição | |  | | --- | |  |  |  | | --- | | Na borda da rede ou entre zonas internas | | |  | | --- | |  |  |  | | --- | | Geralmente em paralelo ao tráfego | | Em linha com o tráfego |
| Resposta | Impede acessos não autorizados com base em regras | Gera alertas, mas **não bloqueia** automaticamente | **Bloqueia automaticamente** ações maliciosas |

1. Uma pessoa lhe procura e pede ajuda sobre formas de proteger as suas senhas. Cite pelo menos três conselhos que você daria a essa pessoa.

Resposta:Use senhas fortes e únicas Crie senhas longas (pelo menos 8 caracteres), combinando letras maiúsculas, minúsculas, números e símbolos. Evite usar informações pessoais e não reutilize a mesma senha em diferentes contas. Ative a autenticação em dois fatores (2FA). Isso adiciona uma camada extra de segurança: mesmo que alguém descubra sua senha, ainda precisará de um segundo código (gerado por app, SMS ou chave física). Use um gerenciador de senhas confiável que armazena e gera senhas seguras para cada conta. Assim, você só precisa lembrar de uma senha-mestre. Exemplos: Bitwarden, senhas (IOS), entre outros.

1. Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

1. A vulnerabilidade

Resposta: Windows falso

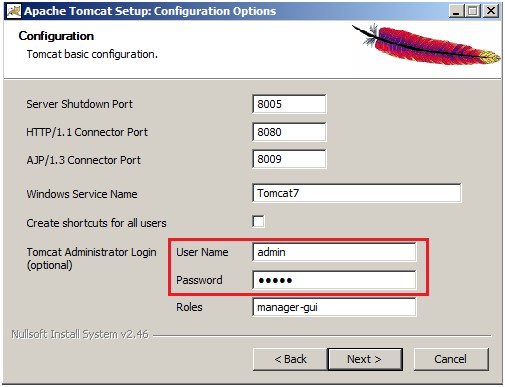
1. A ameaça

Resposta: sujeito a ataques devido a desatualização dos patches oficiais da Microsoft

1. Uma ação defensiva para mitigar a ameaça

Resposta: Baixar um Windows original

7) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

1. A vulnerabilidade

Resposta: Senha e login fracos e usuais

1. A ameaça

Resposta: Login facilmente quebrável

1. Uma ação defensiva para mitigar a ameaça

Resposta: Colocar uma senha e user name mais fortes

8) Ana tem duas mensagens para enviar de forma criptografada para dois amigos: Bob e Carlos. Bob deseja receber a mensagem de maneira que apenas ele possa decifrá-la. Carlos não está preocupado com o sigilo da mensagem, mas deseja ter certeza de que foi mesmo Ana que a enviou. Assuma que todos têm seu par de chaves pública e privada, que todas as chaves públicas são acessíveis. Visando a atender os requisitos de Bob e Carlos, descreva, **em termos de uso das chaves:**

1. como Ana deverá cifrar a mensagem antes de enviar para Bob;

Resposta: Com a chave pública de Bob

1. como Bob deverá decifrar a mensagem de Ana corretamente;

Resposta: Com sua chave privada

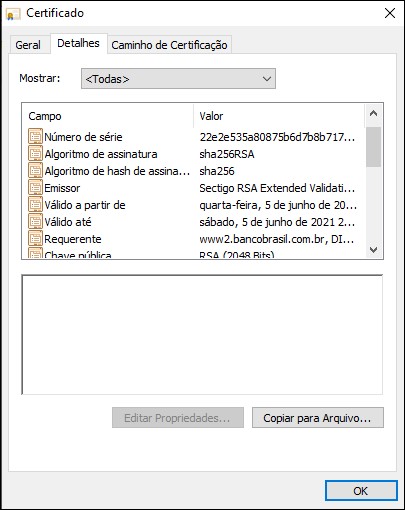
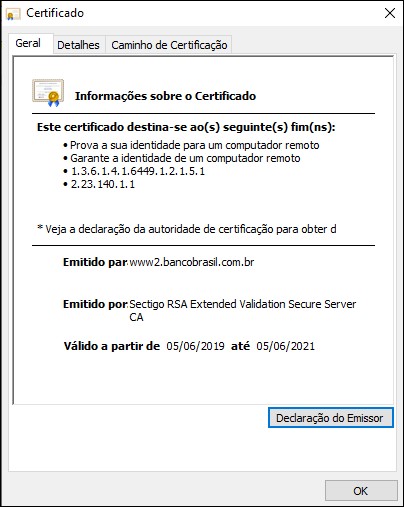
1. como Ana deverá cifrar a mensagem antes de enviar para Carlos;

Resposta: Com sua chave privada

1. como Carlos deverá decifrar a mensagem de Ana corretamente.

Resposta: Com a chave pública de Ana

1. Observe as imagens a seguir:



As imagens apresentam informações do certificado digital do site [www.bb.com.br.](http://www.bb.com.br/) Com base nelas, responda:

* 1. Como se dá a utilização do certificado na origem e no destino? Identifique como são utilizadas as chaves criptográficas do Banco do Brasil.

Resposta: a chave hash SHA256 provê uma chave de origem privada para obter a assinatura digital, para validação, o cliente deve usar a chave pública.

* 1. Cite dois benefícios de segurança que uma transação eletrônica recebe com a utilização do certificado digital do Banco.

Resposta:

- Prova a sua identidade para um computador remoto

- Garante a identidade de um computador remoto

1. Observe a imagem a seguir:



De acordo com a norma ISO 27002: 2013, “convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares”. ABNT (2013).

Cite 3 registros importantes da atividade dos usuários que podem registrados para posterior auditoria de segurança.

1. Uso de privilégios
2. Log de sistema
3. Endereço de protocolo de rede

# Referências

* ABNT (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS). **NBR ISO/IEC 27002:2013**: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2013.

* HINTZGBERGEN, Jule. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. 3. ed. Brasport, Rio de Janeiro, 2018.