**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*?

R: É uma simulação de ataques cibernéticos com o objetivo de identificar vulnerabilidades em sistemas, redes e aplicações. Suas etapas são planejamento que define a estratégia e o que será testado, análise de vulnerabilidade que é atacar e ver como o sistema respondeu ao ataque ,exploração que é ir onde teve a falha e investigar , pós exploração que ve os danos causado pelo o ataque e por ultimo o relatório que manda como os ataques aconteceram e o que deve ser resolvido.

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

R: ICS/OT : Por serem Sistemas de Controle Industrial (ICS) e Tecnologia Operacional (OT) que realiza a gestão de operações físicas, uma simples alteração se torna um erro que pode gerar um impacto enorme na empresa

Rasomware: Sequestra os dados ou sistema de uma empresa, criptografando com uma chave que só o atacante tem ,e em troca pedindo valores absurdos geralmente em criptomoedas para devolver os dados.

DDoS: Um vírus infecta diversos dispositivos, permanece inativo, e loga em um site , com um número absurdo de logs fazendo o site vitima cair

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)?

R: 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.

R: Firewall (parede de fogo) – É uma ação preventiva que controla acessos a rede com base no IP , portas e protocolos .

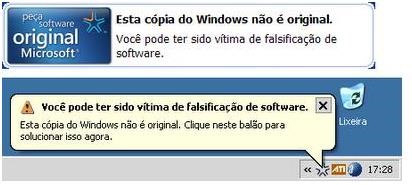
IDS – É uma ação detectiva que monitora acessos e gera alertas quando identifica anormalidades porém não tem ação nenhuma somente os alertas .

IPS –É uma ação preventiva e reativa que bloqueia o acesso estranhos baseado em monitoramento comportamental , quando ele identifica algo que não é comum automaticamente acontece o bloqueio.

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.

R: Use senhas fortes, misturando letras maiúsculas, minúsculas, números e símbolos, nunca repita a mesma senha em vários sites e use um gerenciador de senhas pra guardar tudo com segurança.

1. Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

1. A vulnerabilidade

R: Uso de sistema operacional pirata.

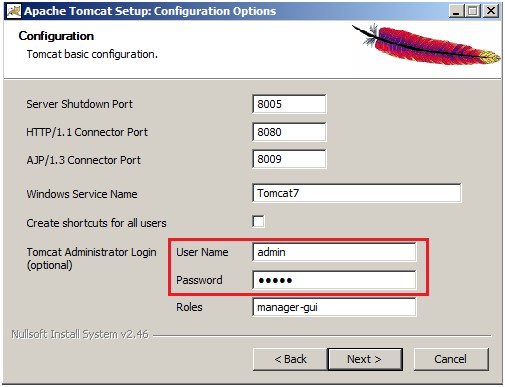
1. A ameaça

R: Maior risco de infecções por malwares, falhas de segurança não corrigidas e acesso não autorizado, já que cópias piratas não recebem atualizações oficiais nem suporte técnico.

1. Uma ação defensiva para mitigar a ameaça

R: Instalar uma versão original e licenciada do sistema operacional, garantindo acesso a atualizações de segurança e suporte oficial.

7) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

1. A vulnerabilidade

R: Uso de nome de usuário e senha fracos ou padrão.

1. A ameaça

R: Invasão por hackers que podem acessar o sistema facilmente.

1. Uma ação defensiva para mitigar a ameaça

R: Criar um nome de usuário e senha fortes e únicos.

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;

R: Ana deve **criptografar a mensagem com a chave pública de Bob**. Assim, só Bob poderá abrir.

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

R: Bob usa **sua chave privada** para decifrar a mensagem que Ana enviou.

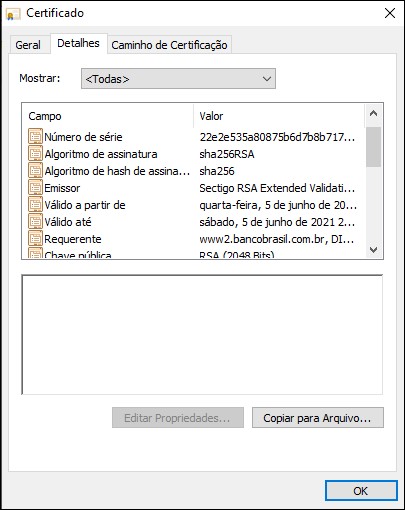
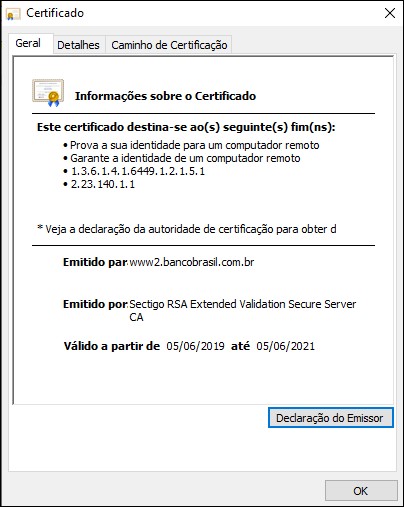
1. como Ana deverá cifrar a mensagem antes de enviar para Carlos;

R: Ana deve **criptografar a mensagem com a sua própria chave privada**.

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

R: Carlos usa a **chave pública de Ana** para verificar que foi realmente ela quem enviou a mensagem.

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.

R: O certificado garante que o site é do Banco do Brasil. O banco usa a chave privada pra proteger os dados e o usuário usa a chave pública pra verificar e mandar as informações seguras.

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

R: Garante que o site é verdadeiro e protege os dados da pessoa pra ninguém mais ver.

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.

R: Horário de login e logout no sistema, arquivos acessados ou modificados e tentativas de acesso não autorizadas.

# 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.