Atividade de revisão

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

Resposta:
Pentest (*penetration test*) é um teste de intrusão que simula ataques reais para identificar vulnerabilidades.
Etapas principais:

1. Varredura
2. Exploração
3. Escalação de privilégios
4. Ocultação.

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

Resposta:
- DDoS (Distributed Denial of Service): sobrecarga de tráfego em servidores, tornando-os indisponíveis.
- Ransomware: criptografa dados e bloqueia acesso até pagamento de resgate, paralisando operações.
- Ataque a infraestrutura elétrica/rede: falhas ou sabotagens em energia ou rede podem derrubar sistemas críticos.

3) 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)?

Resposta:
O conceito é Conformidade (*Compliance*).
Refere-se ao cumprimento de leis, regulamentos internos, obrigações contratuais e normas internacionais.

4) 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.

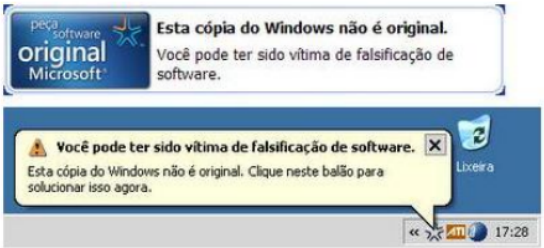
Recurso	Função principal	Características
Firewall	Controle de tráfego	Filtra pacotes entre redes; define regras de acesso; pode ser de rede ou aplicativo.
IDS (Intrusion Detection System)	Detecção	Monitora tráfego e gera alertas sobre atividades suspeitas; não bloqueia, apenas detecta.
IPS (Intrusion Prevention System)	Prevenção	Além de detectar, bloqueia tráfego malicioso em tempo real.

5) 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:

1. Usar senhas fortes (mistura de letras maiúsculas/minúsculas, números e símbolos).
2. Ativar autenticação multifator (MFA).
3. Nunca reutilizar a mesma senha em diferentes serviços e atualizar periodicamente.

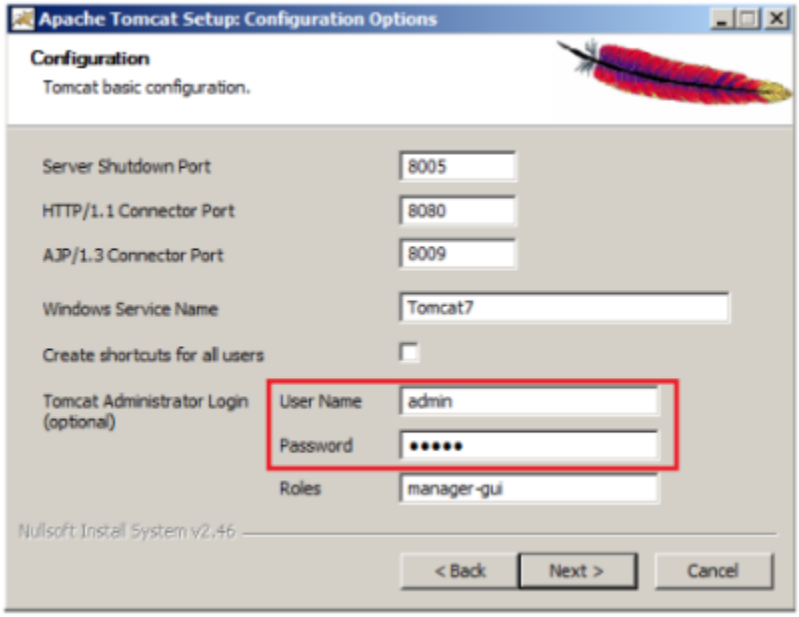
6) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade: **Resposta** -> Uso de software pirata/falsificado.
b) A ameaça: **Resposta:** -> Malware embutido, falhas de atualização e exposição a ataques.
c) Uma ação defensiva para mitigar a ameaça: **Resposta:** -> Utilizar software original/licenciado e manter atualizações automáticas.

7) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade
Resposta: Credenciais padrão fracas (usuário “admin”, senha simples).

b) A ameaça
Resposta: Invasão por brute force ou exploração de credenciais padrão.

c) Uma ação defensiva para mitigar a ameaça
Resposta: Definir senhas fortes, desabilitar contas padrão e aplicar autenticação multifator.

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:

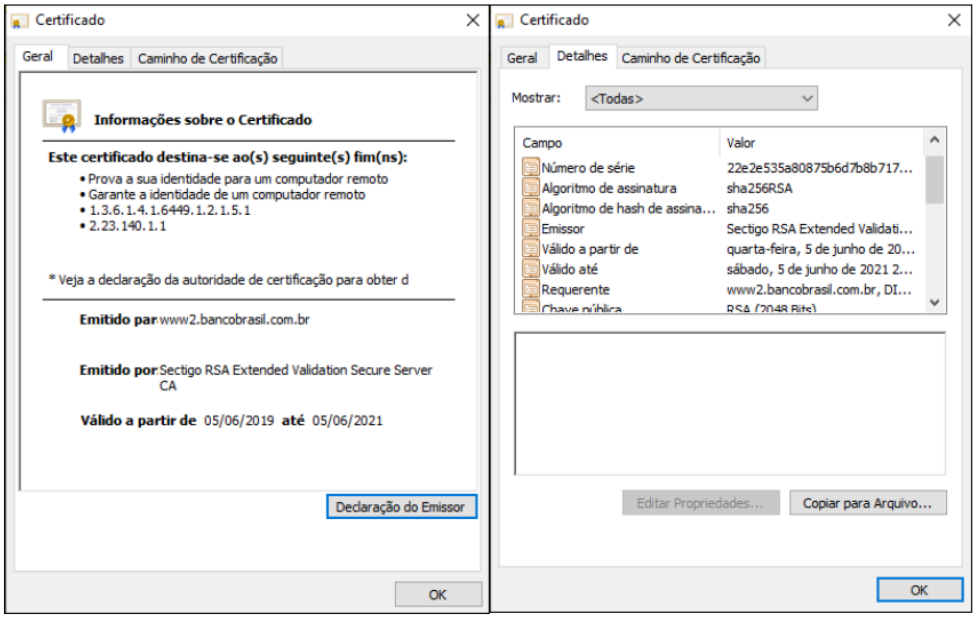
a) como Ana deverá cifrar a mensagem antes de enviar para Bob;
Resposta: Ana → Bob: cifrar com a chave pública de Bob.

b) como Bob deverá decifrar a mensagem de Ana corretamente;
Resposta: Bob: decifrar com sua chave privada.

c) como Ana deverá cifrar a mensagem antes de enviar para Carlos;
Resposta: Ana → Carlos: assinar digitalmente com sua chave privada.

d) como Carlos deverá decifrar a mensagem de Ana corretamente.
Resposta: Carlos: verificar assinatura com a chave pública de Ana.

9) Observe as imagens a seguir:



As imagens apresentam informações do certificado digital do site www.bb.com.br. Com base nelas, responda:

a) Como se dá a utilização do certificado na origem e no destino? Identifique como são utilizadas as chaves criptográficas do Banco do Brasil.
Resposta:
Origem (Banco): usa sua **chave privada** para assinar comunicações.
Destino (usuário): valida assinatura com a **chave pública** do certificado.

b) Cite dois benefícios de segurança que uma transação eletrônica recebe com a utilização do certificado digital do Banco.
Resposta:
Garantia de identidade/autenticidade do site.
Criptografia das transações, protegendo dados contra interceptação.

10) 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.

Resposta:

- Logs de autenticação (login/logout, tentativas falhas).
- Logs de acesso a arquivos e sistemas críticos.
- Logs de alterações administrativas (configurações, permissões, atualizações).