UC Sistemas Computacionais e Segurança – 2025.1
Exercícios de Revisão
Prof. Calvetti

Questões

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

Resposta: Pentest é como um ataque simulado feito por profissionais de segurança para encontrar falhas em algum sistema, rede ou aplicação. O objetivo é descobrir as possíveis vulnerabilidades.

As etapas são:

1. **Planejamento:** definir o que será testado, como e com qual objetivo.
2. **Reconhecimento:** coletar o máximo de informações sobre o alvo.
3. **Varredura e análise:** identificar portas abertas, serviços ativos e possíveis falhas.
4. **Exploração:** tentar invadir de fato, usando as vulnerabilidades encontradas.
5. **Manutenção de acesso:** verificar se seria possível continuar dentro do sistema sem ser percebido.
6. **Relatório:** apresentar todos os achados, riscos e soluções para corrigir as falhas.

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

Resposta: Esse tipo de ataque têm como finalidade derrubar ou travar um sistema, impedindo sua disponibilidade para os usuários:

- **Ataque DDoS (Negação de Serviço Distribuída):** envolve milhares de acessos ao mesmo tempo para sobrecarregar um site ou serviço, fazendo com que ele fique fora do ar.
- **Ransomware:** um tipo de vírus que "sequestra" os dados do sistema, criptografa tudo e só libera mediante pagamento de resgate. Enquanto isso, nada funciona.
- **Botnets:** redes de computadores infectados que são controlados remotamente. Eles podem ser usados para fazer ataques DDoS ou espalhar vírus, comprometendo toda a infraestrutura.

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: A palavra-chave é “Conformidade”, ela serve para representar o compromisso da empresa em seguir leis, regulamentos, políticas internas e contratos. Estar em conformidade é essencial para evitar falhas, multas e até crises de reputação.

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.**

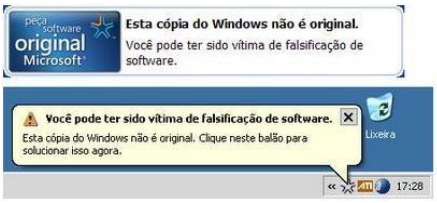
Tecnologia	**O que faz?**	**Como age?**	**Resposta a ameaças**
Firewall	Controla o que entra e sai da rede	Usa regras para permitir ou bloquear conexões	Bloqueia acessos não autorizados
IDS (Sistema de Detecção de Intrusão)	Monitora a rede	Fica observando o tráfego de dados	Só alerta quando detecta algo suspeito
IPS (Sistema de Prevenção de Intrusão)	Monitora e age	Atua como barreira ativa entre a internet e a rede	Detecta e bloqueia o ataque automaticamente

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: Eu diria para:

- Use senhas longas e difíceis de adivinhar: misture letras, números e símbolos. Quanto maior e mais complexa, melhor.
- Ative a verificação em duas etapas (2FA): assim, mesmo que alguém descubra sua senha, ainda precisa de uma segunda confirmação.
- Evite repetir senhas em sites diferentes: se uma for descoberta, todas as outras ficam em risco. Um gerenciador de senhas pode ajudar muito nesse controle.

6) Observe a imagem a seguir.



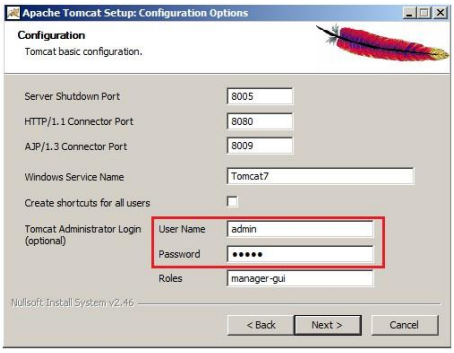
Do ponto de vista da segurança da informação, identifique:

a) **A vulnerabilidade** – O uso de um SO não original pode impedir a instalação de atualizações de segurança e deixar exposto para qualquer tipo de ameaça.

b) **A ameaça** – Risco do usuário cair em golpes e/ou ataques cibernéticos, como instalar programas falsos ou infectados acreditando que estão resolvendo o problema.

c) **Uma ação defensiva para mitigar a ameaça** – Regulariza a cópia do SO, adquirindo a versão original e ativando corretamente

7) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

a) **A vulnerabilidade** – Uso de credenciais muito comuns, conhecidas ou fracas
b) **A ameaça** – Alguma pessoa pode explorar essas credenciais comuns para invadir o sistema, modificar ou até instalar malwares.
c) **Uma ação defensiva para mitigar a ameaça** – Alterar o nome do usuário utilizado e senha por fortes e diferentes, além de autenticação mais robusta, como a em dois fatores.

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:**

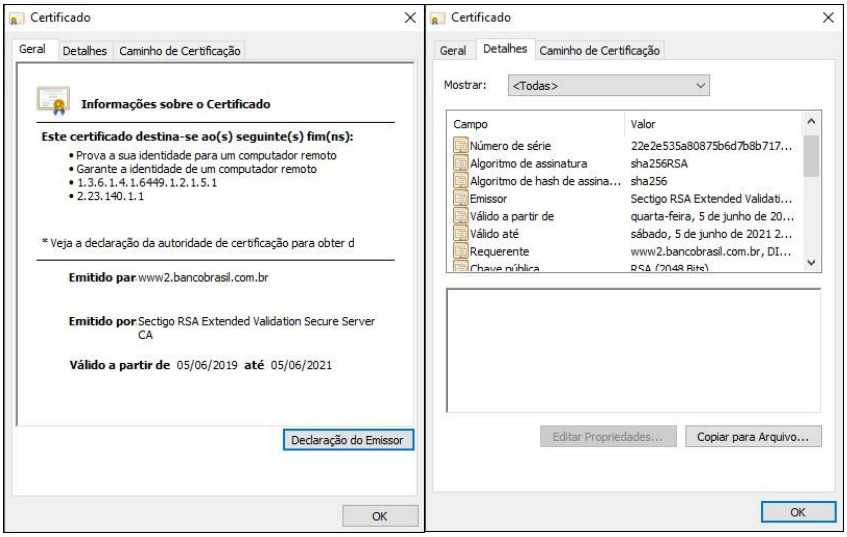
a) como Ana deverá cifrar a mensagem antes de enviar para Bob;
- Ela usa a **chave pública de Bob** para criptografar. Assim, só ele pode abrir.

b) como Bob deverá decifrar a mensagem de Ana corretamente;
- Ele usa a **chave privada dele** para decifrar, já que foi feita com sua chave pública

c) como Ana deverá cifrar a mensagem antes de enviar para Carlos;
- Ela usa a **chave privada dela** para "assinar" a mensagem, garantindo que foi ela quem enviou.

d) como Carlos deverá decifrar a mensagem de Ana corretamente.
- Ele usa a **chave pública de Ana** para confirmar que a assinatura é verdadeira.

9) Observe as imagens a seguir:



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

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

- Na origem o banco utiliza uma chave privada para assinar digitalmente as transações. No destino, mais conhecido como usuário, o navegador checa essa assinatura usando a chave pública do certificado digital.

9.b) Cite dois benefícios de segurança que uma transação eletrônica recebe com a utilização do certificado digital do Banco.

1 - A autenticidade que garante que o site acessado é realmente do BB

2 – A criptografia que protege as informações trocadas entre os clientes e o banco, dificultando uma possível interceptação por terceiros.

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:

- **Tentativas de login e logout no sistema** – Incluindo os horários e se houve algum tipo de falha de autenticação.
- **Acessos a arquivos e dados sensíveis** – Quem acessou, quando e o que foi feito.
- **Alterações em configurações do sistema ou aplicativos** – Como mudanças de permissões ou instalação de novos softwares.

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.