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*?

Resposta:
Um pentest é uma simulação controlada de ataque feita por especialistas em segurança com a intenção de localizar brechas em sistemas, redes ou aplicações. Ele busca identificar fragilidades que possam ser exploradas.

As fases são:

1. **Preparação:** definir o escopo, métodos e metas do teste.
2. **Coleta de dados:** obter o máximo de informações possíveis sobre o alvo.
3. **Análise de vulnerabilidades:** examinar serviços ativos, portas abertas e identificar possíveis falhas.
4. **Tentativa de invasão:** explorar as vulnerabilidades encontradas.
5. **Permanência no sistema:** verificar se seria viável manter o acesso sem ser detectado.
6. **Documentação:** relatar tudo que foi descoberto, os riscos e como corrigir os problemas.

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

Resposta:
Esses ataques têm como propósito tornar o sistema inacessível:

• **Ataque DDoS:** Envolve múltiplos dispositivos acessando simultaneamente um serviço, sobrecarregando-o e deixando-o indisponível.
• **Ransomware:** Um malware que bloqueia o acesso aos dados por meio de criptografia, exigindo pagamento para a liberação.
• **Botnets:** Conjuntos de máquinas infectadas que podem ser usadas remotamente para realizar ataques, como o DDoS.

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:
Conformidade – representa o dever de seguir leis, normas internas, contratos e compromissos legais e regulatórios, sendo fundamental para evitar penalidades e prejuízos à imagem da empresa.

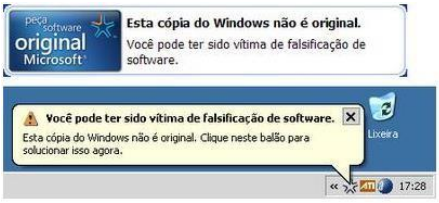
4) Existem vários recursos de software e hardware para estabelecer diversos níveis de segurança em uma rede de computadores. Entre outros, podemos citar os *firewalls* e os sensores (IDS e IPS). Faça um quadro comparativo resumindo as características de cada um dos três recursos.

Tecnologia	Finalidade	Funcionamento	Resposta a Ameaças
Firewall	Controlar o tráfego	Utiliza filtros para permitir ou negar conexões	Bloqueia acessos não permitidos
IDS	Detectar anomalias	Observa o tráfego de dados	Emite alertas ao detectar comportamentos suspeitos
IPS	Prevenir invasões	Atua como barreira proativa	Impede e bloqueia automaticamente as ameaças

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:
- Crie senhas longas e complexas, usando diferentes tipos de caracteres.
- Habilite a autenticação em dois fatores para segurança extra.
- Não reutilize senhas. Use um gerenciador para manter controle.

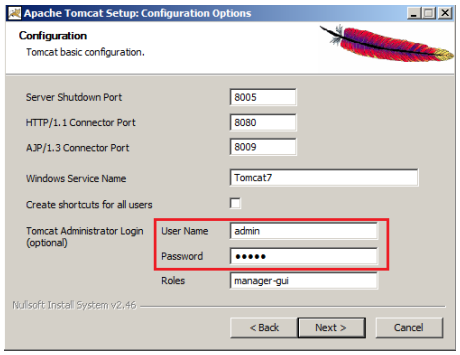
6) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade: Utilização de sistema operacional pirata, que não recebe atualizações de segurança.
b) A ameaça: Risco de infecção por malwares ou golpes através de softwares não confiáveis.
c) Ação preventiva: Adquirir e ativar uma cópia original do sistema operacional para receber atualizações e suporte.

7) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade: Uso de senhas fracas ou padrões previsíveis.
b) A ameaça: Invasão por força bruta ou uso de senhas conhecidas.
c) Uma ação defensiva para mitigar a ameaça: Criar senhas fortes, únicas, e habilitar autenticação em duas etapas.

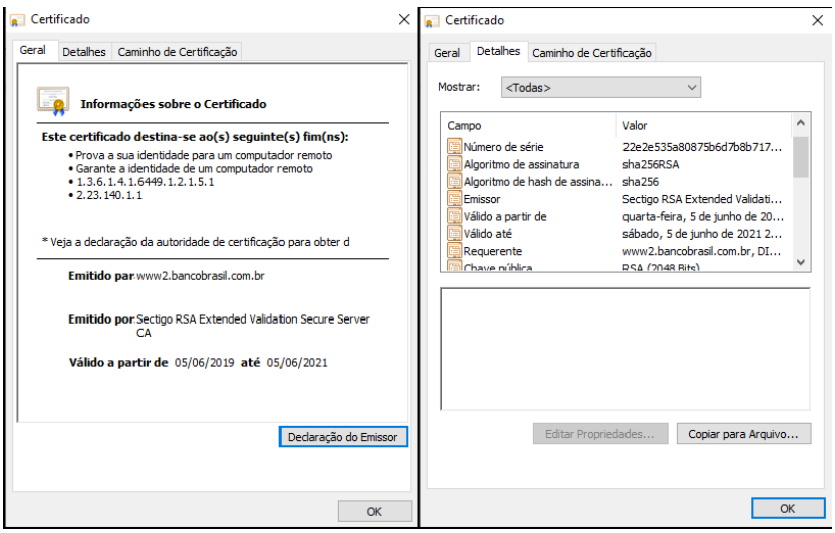
8) Ana tem duas mensagens para enviar de forma criptografada para dois amigos: Bob e Carlos. Bob deseja receber a mensagem de maneira que apenas ele possa decifrá-la. Carlos não está preocupado com o sigilo da mensagem, mas deseja ter certeza de que foi mesmo Ana que a enviou. Assuma que todos têm seu 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;
b) como Bob deverá decifrar a mensagem de Ana corretamente;
c) como Ana deverá cifrar a mensagem antes de enviar para Carlos;
d) como Carlos deverá decifrar a mensagem de Ana corretamente.

Resposta:

a) Ana deve usar a **chave pública de Bob** para cifrar a mensagem, garantindo que só ele possa decifrar.
b) Bob usará sua **chave privada** para decifrar a mensagem enviada.
c) Para Carlos, Ana deve assinar a mensagem com sua **chave privada**, garantindo a autoria.
d) Carlos usará a **chave pública de Ana** para verificar se a mensagem veio realmente dela.

9) Observe as imagens a seguir:



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

10) Como se dá a utilização do certificado na origem e no destino? Identifique como são utilizadas as chaves criptográficas do Banco do Brasil.
Resposta: Autenticidade do site garantida, evitando fraudes.

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

Resposta: Confidencialidade das informações trocadas por meio da criptografia, protegendo contra interceptações.

11) 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:

1. Tentativas de login e logout, com horário e resultado (sucesso ou falha).
2. Acessos a arquivos sensíveis, identificando quem acessou e quando.
3. Modificações em configurações do sistema ou instalação de novos programas.

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.