**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*?

**Pentest (Teste de Penetração) é uma simulação controlada de ataque cibernético feita por profissionais de segurança para identificar vulnerabilidades em sistemas, redes ou aplicações antes que atacantes reais as explorem.**

**Etapas:**

**Planejamento e Reconhecimento;**

**Varredura;**

**Ganho de Acesso;**

**Manutenção de Acesso;**

**Remoção de Vestígios e Relatório.**

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

**DDoS (Distributed Denial of Service):**

**Ataque que sobrecarrega o servidor com múltiplas requisições simultâneas vindas de várias máquinas.**

**Resultado: o sistema fica inacessível para usuários legítimos.**

**Ransomware:**

**Malware que criptografa arquivos ou bloqueia o sistema, exigindo pagamento para liberação.**

**Resultado: os recursos ficam indisponíveis até a restauração ou pagamento.**

**Sabotagem Física ou Lógica:**

**Desligamento proposital de servidores, exclusão de dados ou rompimento de redes.**

**Resultado: impacta diretamente a continuidade dos serviços.**

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)?

**Compliance.**

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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Recurso** | **Função Principal** | **Atua em Tempo Real?** | **Atua Passivamente?** | **Atua Ativamente?** |
| **Firewall** | **Filtra tráfego com base em regras** | **Sim** | **Não** | **Sim** |
| **IDS** | **Detecta atividades suspeitas** | **Parcialmente** | **Sim** | **Não** |
| **IPS** | **Detecta e bloqueia ameaças** | **Sim** | **Não** | **Sim** |

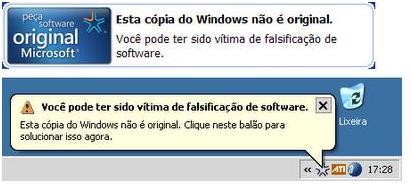
5) Uma pessoa lhe procura e pede ajuda sobre formas de proteger as suas senhas. Cite pelo menos três conselhos que você daria a essa pessoa.

**Use senhas fortes e únicas: combinação de letras maiúsculas, minúsculas, números e símbolos;**

**Ative autenticação de dois fatores (2FA) sempre que possível;**

**Nunca compartilhe suas senhas e evite anotá-las em lugares públicos ou digitais desprotegidos.**

6) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

1. A vulnerabilidade

**Quando um sistema não é original, ele pode não receber atualizações de segurança, ficando exposto a falhas conhecidas, sem correções disponibilizadas pela Microsoft.**

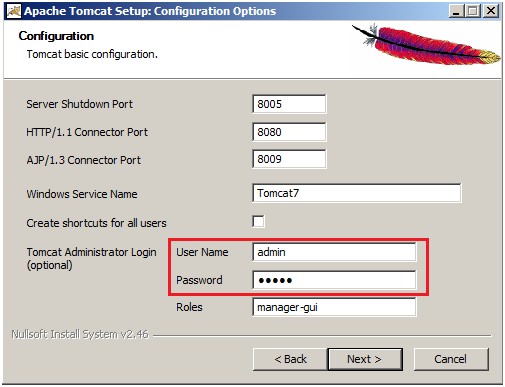
1. A ameaça

**Exploração de vulnerabilidades por malwares, hackers ou códigos maliciosos, aproveitando brechas não corrigidas no sistema pirata.**

1. Uma ação defensiva para mitigar a ameaça

**Utilizar software original e licenciado diretamente de fontes confiáveis.**

7) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

1. A vulnerabilidade

**Essas credenciais são previsíveis e frequentemente são alvos de ataques automatizados.**

1. A ameaça

**Acesso não autorizado ao painel de administração do servidor.**

1. Uma ação defensiva para mitigar a ameaça

**Alterar o nome de usuário padrão e utilizar uma senha forte e complexa.**

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;

**Ana deve criptografar a mensagem com a chave pública de Bob.**

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

**Bob deve usar sua chave privada para decifrar a mensagem.**

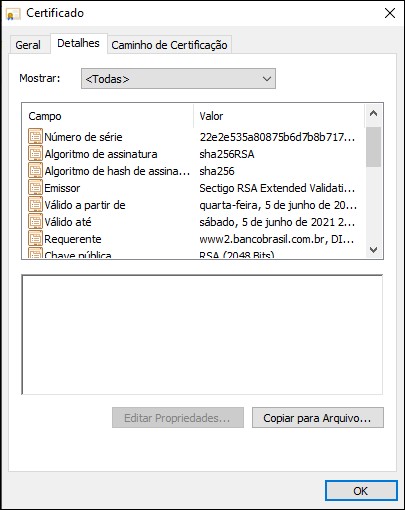
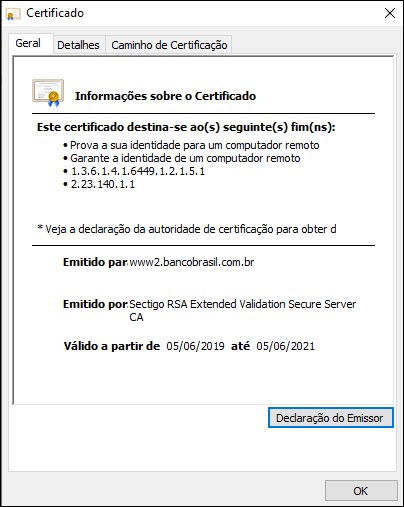
1. como Ana deverá cifrar a mensagem antes de enviar para Carlos;

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

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

**Carlos usará a chave pública de Ana para decifrar 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.

**Banco do Brasil (origem): Usa a chave privada para assinar dados e descriptografar mensagens.**

**Cliente (destino): Usa a chave pública (do certificado) para:**

**Verificar se o site é verdadeiro;**

**Criptografar dados antes de enviar.**

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

**Prova que o site é verdadeiro (não é um golpe);**

**Protege os dados (ninguém consegue espionar ou alterar as informações durante a transação).**

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.

**Logs de Acesso;**

**Logs de Tentativas de Login;**

**Logs de Alterações em Dados Críticos.**

# 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.