USJT – UC Sistemas Computacionais e Segurança – Prof. Calvetti
Aluno: Daniel Silva

ATIVIDADE 3:

Questões

1) O que é um pentest? Quais são as etapas de um pentest?
R: Pentest (penetration test), é um teste de segurança cibernética que utiliza um ataque cibernético simulado para encontrar vulnerabilidades em um sistema computacional. As etapas são: reconhecimento, descoberta e desenvolvimento de alvos, invasão, escalada de privilégios e limpeza e geração de relatórios

IBM. **O processo de testes de penetração**. Disponível em <https://www.ibm.com/br-pt/think/topics/penetration-testing>. Acesso em 11 set. 2025.

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

R: - DDoS: Utilização de uma rede de bots que sobrecarregam servidores com uma inundação de solicitações simultâneas, esgotando os recursos do alvo e impedindo acesso de usuários legítimos.
- Ransomware: Criptografa arquivos que impede o acesso a dados ou sistemas.
- Teardrop: DoS que explora uma falha em sistemas operacionais mais antigos enviando pacotes de dados IP fragmentados de forma maliciosa, de maneira que o sistema-alvo não consegue remontar corretamente, causando falhas e travamentos.

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)?

R: Legalidade.

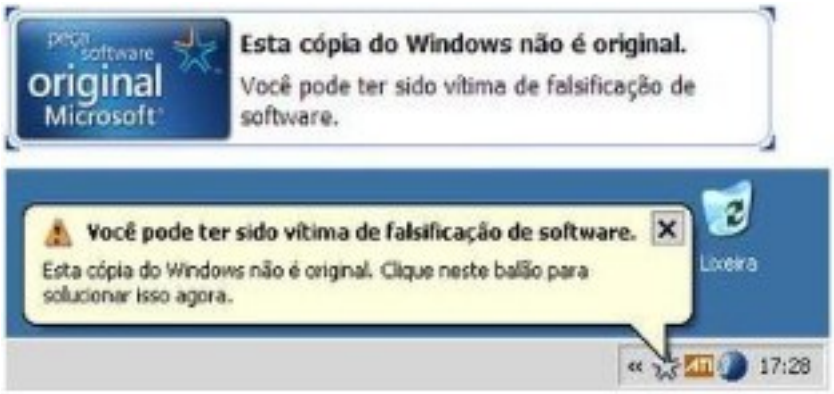
4) Existem vários recursos de software e hardware para estabelecer diversos níveis de segurança em uma rede de computadores. Entre outros, podemos citar os firewalls e os sensores (IDS e IPS). Faça um quadro comparativo resumindo as características de cada um dos três

Característica	Firewall	IDS (Sistema de Detecção de Intrusão)	IPS (Sistema de Prevenção de Intrusão)
Função Principal	Barreira de **filtro** de tráfego.	**Monitoramento** e **alerta** de tráfego suspeito.	**Prevenção** e **bloqueio** ativo de tráfego malicioso.
Modo de Operação	Filtra pacotes com base em **regras** (IP, porta, protocolo) para permitir ou negar a passagem.	Analisa cópias do tráfego (geralmente fora de linha) em busca de **assinaturas** ou **anomalias**.	Analisa o tráfego **em linha** (in-line) e, se detectada uma ameaça, toma ações imediatas.
Ação em Caso de Ameaça	Bloqueia o tráfego que **viola as regras** configuradas.	**Gera alertas** e registra informações, mas **não bloqueia** o tráfego ativamente.	**Bloqueia** o pacote ou a conexão, **encerra a sessão** ou aplica outras medidas de **contenção**.
Localização Típica	Atua como **ponto de entrada/saída** principal da rede.	Fica tipicamente **fora do caminho** direto do tráfego de rede (offline ou passivo).	Fica **em linha** com o fluxo de tráfego (inline ou ativo), geralmente após o firewall.
Impacto no Desempenho	Geralmente baixo, pois foca em cabeçalhos de pacotes ou estados de conexão.	Baixo impacto, pois analisa cópias do tráfego.	Pode ter um impacto maior, pois realiza inspeção profunda (DPI) e deve agir antes que o tráfego chegue ao destino.

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.

R: Use bastante quantidade de caracteres (no mínimo 16); essa senha deve possuir símbolos, números, letras maiúsculas e minúsculas; não guarde sua senha em um lugar que qualquer pessoa tenha acesso (a princípio, decore); não use a mesma senha para tudo; entre outros.

6) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade

R: Sistema operacional não original, ou seja, não recebe atualizações e está alterado.

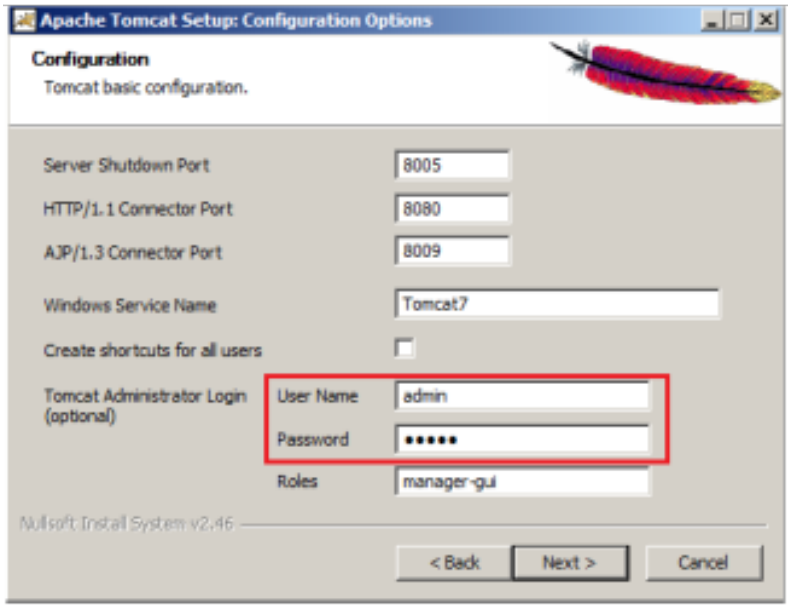
b) A ameaça

R: Esse software, por não ser corrigido, por ser infectado por malwares.

c) Uma ação defensiva para mitigar a ameaça

R: Utilizar uma cópia legítima desse sistema operacional.

7) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade

R: Usuário comum “admin” e senha pequena.

b) A ameaça
R: Um criminoso pode usar força bruta para conseguir acesso ao sistema

c) Uma ação defensiva para mitigar a ameaça
R: Renomear os usuários administradores e aumentar o número de caracteres da senha.

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;
R: Utilizando a chave pública de Bob.

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

d)como Ana deverá cifrar a mensagem antes de enviar para Carlos;
R: Utilizando sua chave privada.

e) como Carlos deverá decifrar a mensagem de Ana corretamente.
R: Utilizando a chave pública de Ana.

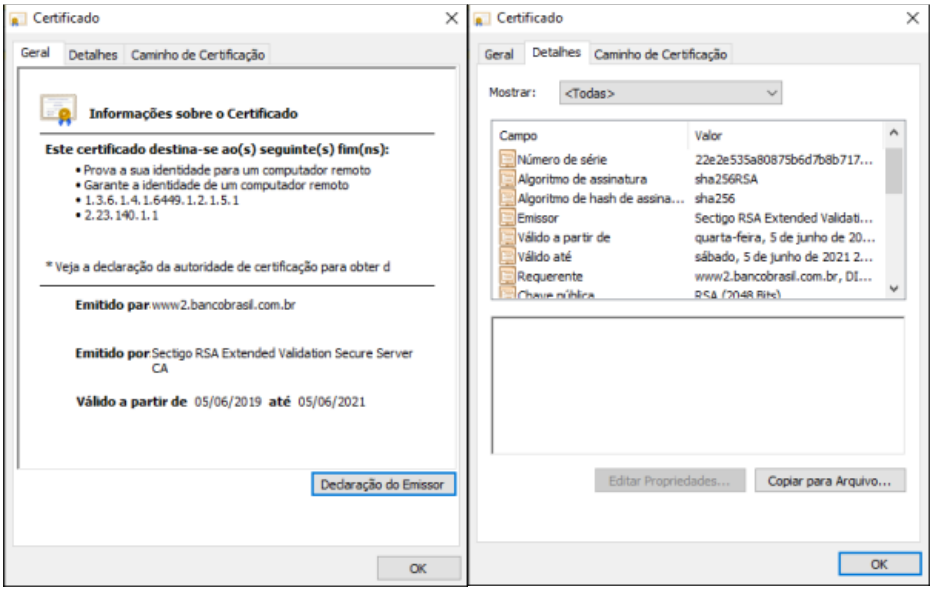
9) Observe as imagens a seguir.

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

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.

R: - A CA Serctigo gera um resumo criptográfico (hash) dos dados do Banco.
- O Banco criptografa o hash com sua chave privada (assinatura digital).
- O cliente do banco decifra o hash com a chave pública do Banco.
- O cliente do banco compara o hash da mensagem enviada com o hash que estava criptografado
- Se eles coincidirem, então a mensagem foi validada.

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



R: Autenticidade, integridade e não-repúdio.

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.
R: A identificação do usuário; data e hora de sua entrada e saída; registro de uso de privilégios; registro de alteração de arquivos; entre outros.

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.