QUESTÕES DE REVISÃO

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

Pentest, ou teste de penetração, é uma forma de avaliar a segurança de um sistema simulando ataques que permitem que você identifique vulnerabilidades dentro desse ambiente.

Para que o pentest seja eficaz, é necessário seguir 6 etapas:

1 - Descobrir: a fase inicial, onde é levantado os requisitos do sistema para que o pentester (aquele que irá realizar o teste de penetração) entenda com que tipo de ambiente está lidando.

2 - Planejar: o objetivo principal dessa fase é achar o profissional que irá realizar o pentest. É importante que ele tenha conhecimento atualizado de tecnologias para que o sistema também possua, ao final de todas as etapas, a melhor segurança possível para o momento.

3 - Testar: onde o pentester irá realizar o seu trabalho, reunindo todas as informações obtidas na etapa 1 para achar possíveis vulnerabilidades existentes no sistema.

4 - Remediar: com o pentest ainda em andamento, o profissional irá comunicar a empresa as informações adquiridas pelo teste, para que a mesma comece a providenciar resoluções para essas vulnerabilidades.

5 - Relatar: com o pentest acabado, deve ser criado um relatório contendo a forma como o teste de intrusão foi feito, quais vulnerabilidades foram encontradas e quaisquer outras informações que a pessoa responsável pelo teste ache importante.

6 - Analisar: finalmente, a empresa e o pentester devem analisar os dados obtidos e começar a trabalhar na segurança do sistema conforme o que a análise do relatório sugere.

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

Ataque DDoS (Distributed Denial of Service, ou Negação de Serviço): sobrecarrega o sistema com uma enorme quantidade de solicitações, estas que normalmente chegam de computadores infectados por malware, ou também chamados de computadores zumbis. Essas solicitações derrubam o sistema, impedindo que qualquer usuário o acesse.

Ransomware: esse tipo de ataque infecta um sistema, sequestra e criptografa os seus dados, e o acesso fica bloqueado até que alguém pague o resgate dos dados. O ataque é praticamente ineficaz se a vítima possui backup do sistema, pois assim é necessário apenas instalar novamente o sistema operacional, mas dependendo de quando foi feito o backup, o prejuízo pode ser grande.

Ataques internos: funcionários ou pessoas com acesso ao sistema de uma determinada empresa podem desligar ou danificar o servidor, fazendo com que o sistema fique indisponível. Novamente, se a empresa tiver o backup recente da plataforma, o ataque é ineficaz.

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)?

Conformidade.

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.

	Firewall	**IDS**	**IPS**
Função principal	Controlar o tráfego	Detectar e monitorar intrusões	Detectar e monitorar intrusões, porém também se previne
Ação	Bloquear ou permitir tráfego	Gerar alertas	Bloquear tráfego, gerar alertas
Tipo de análise	stateful ou stateless	Baseado em assinaturas, anomalias ou híbrido	Baseado em assinaturas, anomalias ou híbrido
Proatividade	Baixa	Média	Alta

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.

Existem vários conselhos que você pode fornecer como uma forma para proteger suas senhas, aqui estão alguns deles:

- Autenticação de múltiplos fatores.
- Trocar a senha regularmente, 1 ou 2 anos para uso pessoal, e a cada 4 meses para uso empresarial.
- Nada de senhas com informações pessoais, seriam as primeiras senhas testadas pelos crackers.
- A utilização de um gerenciador de senhas.

6) Observe a imagem a seguir.

Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade

O sistema operacional não é original, portanto não receberá futuras atualizações e correções.

b) A ameaça

Por não ser um sistema operacional original, o risco de adquirir um software malicioso é maior.

c) Uma ação defensiva para mitigar a ameaça

Trocar o sistema operacional por um legítimo ou usar um open source, como Linux.

7) Observe a imagem a seguir.

Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade

A senha contém apenas cinco caracteres, sendo extremamente fraca e de fácil descoberta. Além do nome “Admin” que é padrão em vários sistemas.

b) A ameaça

Um cracker consegue descobrir a senha com mais facilidade.

c) Uma ação defensiva para mitigar a ameaça

Trocar o nome de todos os usuários administrativos e melhorar as senhas.

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;

Deverá cifrar com a chave pública de Bob.

b) como Bob deverá decifrar a mensagem de Ana corretamente;

Deverá decifrar com a sua chave privada.

c) como Ana deverá cifrar a mensagem antes de enviar para Carlos;

Deverá cifrar com a sua chave privada.

d) como Carlos deverá decifrar a mensagem de Ana corretamente.

Deverá decifrar 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:
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.

O Banco do Brasil usa criptografia com duas chaves (assimétrica). O servidor do banco (origem) envia um certificado com sua chave pública para o cliente. O cliente usa essa chave para criptografar as informações que serão enviadas ao banco. Apenas o Banco do Brasil, com sua chave privada, consegue descriptografar essas informações e acessá-las. Ou seja, o cliente usa a chave pública para enviar dados seguros, e o banco usa a chave privada para ler esses dados.

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

Segurança dos dados: A criptografia protege as informações trocadas entre o cliente e o Banco do Brasil, garantindo que ninguém possa ler ou alterar os dados durante a transmissão.

Confirmação de identidade: O certificado digital garante que o cliente está acessando o verdadeiro site do Banco do Brasil, evitando fraudes e ataques, já que o certificado é emitido por uma organização confiável.

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 ser registrados para posterior auditoria de segurança.

De acordo com a ISO 27002:2013, três registros importantes das atividades dos usuários que podem ser mantidos para auditorias de segurança incluem:

1. Tentativas de login, tanto as bem-sucedidas quanto as fracassadas – É essencial registrar quando um usuário tenta entrar no sistema, seja com sucesso ou falhando, para identificar possíveis acessos indevidos ou comportamentos suspeitos.

2. Acesso a informações confidenciais ou sistemas críticos – Registros que rastreiam quando um usuário acessa ou altera dados sensíveis ou sistemas importantes ajudam a garantir que apenas pessoas autorizadas tenham acesso.

3. Alterações nas permissões de acesso ou configurações de segurança – Qualquer mudança nas permissões de usuários ou nas configurações de segurança deve ser registrada, pois modificações não autorizadas podem comprometer a segurança do sistema.