Questões

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

Pentest (Teste de penetração), é um processo para avaliar a segurança de um sistema realizando vários ataques para identificar as vulnerabilidades do sistema.

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

Ataque DDOS (Ele sobrecarrega o servidor evitando que usuários reais possam acessar o site)

Ransomware (O criminoso trava o sistema ou criptografa os arquivos e só libera se a vítima pagar)

Wiper Malware (Ao invés de travar os arquivos como no ransomware, ele destrói tudo**)**

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)?

Sim**,** 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 = Controla o tráfego de rede (entrada/saída). Ele age como uma *barreira de proteção*, controlando o que entra e o que sai.

IDS (Sistema de Detecção de Intrusão) = Detecta atividades suspeitas. O **IDS** não bloqueia nada, só fica “observando” o tráfego da rede, como um *sensor de alarme*. Se detectar algo estranho, ele avisa, mas não age sozinho.

IPS (Sistema de Prevenção de Intrusão) = Detecta e bloqueia ameaças em tempo real. Ativo. Ele também detecta ameaças, mas já toma uma ação automática, como bloquear ou derrubar a conexão suspeita.

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.

1. Criar senhas fortes como: S3NH@F0RT3!14g00gl3
2. Usar senhas variadas para diferentes sites.
3. Trocar as senhas ocasionalmente e se atentar se elas não foram vazadas na DeepWeb.

6) Observe a imagem a seguir.

Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade = O software do usuário pode não ser original.

b) A ameaça = Por não ser original (clonado) não existe proteção e segurança com os dados dele.

c) Uma ação defensiva para mitigar a ameaça = Instalar um novo software original, formatar o PC para evitar que tenha um malware spyware, já que não pode ser retirado apenas desinstalando o programa.

7) Observe a imagem a seguir.

Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade = Utilização de um nome de usuário padrão (`admin`) e configuração de senha durante a instalação, o que pode indicar uma senha fraca ou padrão (password ou admin). Além disso, exibir a configuração de senha na instalação pode facilitar vazamentos caso a tela seja exposta ou capturada.

b) A ameaça = Um atacante pode explorar essa vulnerabilidade realizando um ataque de força bruta ou tentando senhas padrão para obter acesso administrativo ao servidor Tomcat, comprometendo o sistema.

c) Uma ação defensiva para mitigar a ameaça =

Alterar o nome de usuário padrão para algo menos previsível, utilizar uma senha forte., restringir o acesso ao painel de administração por IP ou via firewall, desabilitar contas administrativas padrão se não forem necessárias e utilizar autenticação multifator (MFA).

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;

Ana usa a chave pública de Bob para criptografar a mensagem.

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

Bob usa sua chave privada para decifrar a mensagem criptografada com sua chave pública.

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

Ana usa sua chave privada para assinar digitalmente a mensagem.

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

Carlos usa a chave pública de Ana para verificar a assinatura.

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 certificado digital é usado para autenticação, integridade e confidencialidade em transações eletrônicas.

Na origem (cliente): O cliente usa seu certificado digital para assinar digitalmente a transação, garantindo sua identidade e a integridade dos dados.

No destino (Banco do Brasil): O banco utiliza a chave pública para verificar a assinatura digital do cliente, assegurando que a transação não foi alterada.

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

Autenticação: Garante que as partes envolvidas na transação (cliente e banco) sejam autenticadas de forma segura.

Integridade e Não Repúdio: Assegura que os dados não foram alterados durante a transmissão e que nenhuma das partes pode negar a transação, pois a assinatura digital é única e vinculada à chave privada.

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.

Registro de entrada e saída no sistema.
Registro de alteração no sistema como alteração de arquivos, documentos e afins…
Registro de comandos realizados.
Registro de arquivos acessados.