Nome: Rafaela Maria da Silva  
RA: 825134501  
Professor: Robson Calvetti  
  
Exercícios de Revisão  
1) O que é um pentest? Quais são as etapas de um pentest?

R: Pentest é um método para identificar as vulnerabilidades de um sistema.  
As etapas consistem em definir o objetivo, as limitações e quais serão os sistemas teste, encontrar possíveis pontos de entrada, utilizar ferramentas analisando as vulnerabilidades, testar as falhas para identificar os impactos de um real ataque, caso haja falhas, tentar obter acesso elevado para ver quais são os riscos, documentar os riscos e sugerir correções, por último aplicar novas medidas e fazer novos testes para ver se as falhas foram resolvidas.

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

R: 1 -Ataque de DDoS: Sobrecarregamento de um servidor com um grande volume solicitações, isso faz com que o sistema funcione com lentidão ou fique indisponível para os usuários.  
2 – Ransomware: Um malware que criptografa arquivos e exige pagamento para restaurar o acesso, isso pode paralisar o uso de um sistema.  
3 – Ataque a infraestrutura física: Um invasor altera a configuração de uma rede bloqueando os acessos ao sistema, isso faz que o sistema fique indisponível até que uma equipe técnica possa resolver o problema.

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: 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.

R:

|  |  |  |  |
| --- | --- | --- | --- |
| Recurso | Tipo | Função | Características |
| Firewall | Hardware/ Software | Controla o tráfego de rede. | Filtra pacotes de dados, bloqueia acessos não autorizados, define regras de segurança. |
| IDS | Software/ Hardware | Monitora e detecta ameaças. | Identifica atividades suspeitas, alerta administradores, não bloqueia ataques automaticamente. |
| IPS | Software/ Hardware | Previne ataques. | Atua como IDS, mas também bloqueia tráfego malicioso, pode modificar pacotes e interromper conexões perigosas. |

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 senhas fortes e únicas, ative a autentificação de dois fatores, não compartilhe suas senhas e nem reutilize a mesma senha em vários sistemas.

6) Observe a imagem a seguir.

Interface gráfica do usuário, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade  
R: O uso de uma cópia não original do Windows, pode não receber atualizações de segurança e suas devidas correções.

b) A ameaça

R: A possibilidade de ataques cibercriminosos pois não há a proteção adequada, como malware, acesso não autorizado e comprometimento de dados.

c) Uma ação defensiva para mitigar a ameaça  
R: Utilizar a versão legitima do Windows que é segura, tem um suporte oficial e proteção contra ameaças.

7) Observe a imagem a seguir.

Interface gráfica do usuário

O conteúdo gerado por IA pode estar incorreto.

Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade  
R: A exibição das credenciais de login do administrador na tela de configuração do Apache Tomcat. Isso pode permitir que qualquer pessoa com acesso visual obtenha essas informações.

b) A ameaça  
R: Um usuário não autorizado visualizar e utilizar essas credenciais para acessar o sistema Tomcat, podendo causar danos à segurança dos dados e do servidor.

c) Uma ação defensiva para mitigar a ameaça  
R: Criptografar as credenciais e restringir o acesso da tela de configuração apenas a usuários autorizados, podendo também adicionar autentificação de dois fatores para reforçar a segurança.

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: Ana deve cifrar a mensagem usando a chave pública de Bob.

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

c) como Ana deverá cifrar a mensagem antes de enviar para Carlos;  
R: Ana deve assinar digitalmente a mensagem usando sua chave privada.

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

R: Carlos deve usar a chave pública de Ana para verificar a assinatura digital e confirmar que a mensagem foi realmente enviada por ela.

9) Observe as imagens a seguir:

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

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: O processo utilizado é de criptografia assimétrica.  
Origem: O site possui um certificado digital emitido por uma autoridade certificadora confiável e o servidor utiliza sua chave privada para proteger a comunicação e autenticar sua identidade. Destino: O navegador do usuário verifica a chave pública do certificado do Banco do Brasil, garantindo que a conexão é legítima e a comunicação é criptografada com essa chave pública, impedindo que terceiros interceptem dados sensíveis.

9.b) Cite dois benefícios de segurança que uma transação eletrônica recebe com a utilização do certificado digital do Banco.  
R: Confidencialidade pois a criptografia impede que dados, como senhas e informações bancárias, sejam acessadas por invasores durante a comunicação. E a autenticidade pois o certificado digital garante que o usuário está realmente acessando o site oficial do Banco do Brasil e não um site falso criado para golpes.

10) Observe a imagem a seguir:

Texto

O conteúdo gerado por IA pode estar incorreto.

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: Registro de login e logout pois consegue identificar quando um usuário acessa e sai do sistema, ajudando a detectar acessos não autorizados ou padrões suspeitos. Tentativas de acesso não autorizado pois registra falhas de login, possíveis ataques de força bruta e tentativas de invasão. Alterações em sistemas e dados pois indica quem realizou modificações em arquivos ou configurações críticas, garantindo rastreabilidade e responsabilidade.