PRÁTICA 07

EXERCÍCIO - 1

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

R: O teste de intrusão, ou pentest, é uma técnica proativa e controlada utilizada para avaliar a segurança de sistemas, redes, aplicativos e ambientes tecnológicos como um todo. O objetivo principal de um pentest é simular os métodos e técnicas que um atacante real poderia empregar para explorar vulnerabilidades e invadir sistemas. No entanto, ao contrário de um ataque real, um pentest é conduzido de forma ética, legal e controlada, com o objetivo de identificar falhas de segurança antes que sejam exploradas por criminosos cibernéticos.

Basicamente, um indivíduo ou equipe irá testar a segurança do alvo literalmente tentando invadi-lo, como um hacker faria numa situação real, com a diferença que nesses casos, é dada uma permissão para tal tentativa

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

R:. DoS (Negação de Serviço): Ataque que sobrecarrega um sistema ou servidor com um volume excessivo de requisições, esgotando seus recursos e tornando-o indisponível para os usuários legítimos.

DDoS (Negação de Serviço Distribuída): Similar ao DoS, mas realizado a partir de várias máquinas distribuídas (geralmente infectadas por malware). Isso torna o ataque mais difícil de ser bloqueado, causando sobrecarga no sistema e queda do serviço.

Ransomware: Malware que criptografa os dados do sistema ou bloqueia o acesso, exigindo um resgate. Isso afeta diretamente a disponibilidade, já que o acesso ao sistema ou dados fica indisponível até que seja resolvido.

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: Confidencialidade;

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:

   Firewall:

   - Controla o tráfego de rede com base em regras predefinidas.
   - Atua como uma barreira entre redes internas seguras e redes externas (como a internet).
   - Foca principalmente na filtragem de pacotes, bloqueando ou permitindo o tráfego com base em critérios.
   - Não detecta ou impede ataques, mas bloqueia portas e serviços conforme as regras de configuração.

   IDS:

   - Sistema de detecção de intrusões que monitora e analisa o tráfego de rede em busca de atividades suspeitas.
   - Apenas alerta o administrador sobre possíveis ataques ou violações, sem tomar ações preventivas.
   - Trabalha de forma passiva, analisando o tráfego e gerando logs e alertas.

   IPS:

   - Sistema de prevenção de intrusões que não só detecta, mas também bloqueia ativamente ameaças.
   - Inspeciona o tráfego e, ao detectar anomalias, automaticamente toma medidas para prevenir ataques.

- Atua de forma ativa, interferindo no tráfego de rede para interromper atividades maliciosas.

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: Atualizar constantemente as senhas; usar senhas longas com caracteres especiais e letras maiúsculas e minúsculas; não usar senhas simples como data de aniversário.

6. Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade: Uma cópia não original pode conter falhas de segurança e deixar o sistema vulnerável;

b) A ameaça: Maior vulnerabilidade na segurança e baixo desempenho a longo prazo;

c) Uma ação defensiva para mitigar a ameaça: Uma ação defensiva para mitigar a ameaça: Desinstalar a versão não original do Windows e instalar uma oficial.

7. Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade: Senha padrão do equipamento;

b) A ameaça: Senha fácil de ser descoberta por possíveis invasores;

c) Uma ação defensiva para mitigar a ameaça: Alterar a senha do equipamento

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 deverá cifrar a mensagem com um sistema de criptografia assimétrica, entregando a chave privada ao Bob e ficando com a chave pública

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

R: Bob deverá decifrar a mensagem de Ana com a chave privada;

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

R: Ana deverá cifrar com sua chave;

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

R: Carlos deverá decifrar com a chave pública de Ana

9. 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 Certificadora Serctigo cria um resumo dos dados do banco usando uma função de hash, que gera uma impressão digital única da informação. Esse resumo (hash) é então criptografado com a chave privada do banco, resultando na assinatura digital.

Para verificar a autenticidade dessa assinatura, o cliente do banco utiliza a chave pública do banco, encontrada no certificado, para decifrá-la. Após isso, o cliente também calcula o hash da mensagem recebida. Se o hash gerado pelo cliente for igual ao hash decifrado da assinatura digital, isso confirma que a mensagem é válida e não foi alterada.

Isso garante a integridade e a autenticidade da mensagem.

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

R: A autenticação da origem garante que as mensagens recebidas realmente vêm da fonte indicada no certificado, neste caso, o Banco do Brasil.

A integridade assegura que as mensagens do Banco do Brasil chegaram sem modificações, ou seja, não foram alteradas acidentalmente ou de forma maliciosa.

Além disso, há o princípio de não-repúdio, que impede o banco de negar que enviou as mensagens, garantindo que ele assuma a responsabilidade por elas.

10) 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: Tentativas de login (sucesso e falha): Monitorar as tentativas de login bem-sucedidas e falhas ajuda a identificar possíveis acessos não autorizados ou tentativas de ataque, como força bruta.

Alterações de configurações ou permissões: Qualquer mudança nas configurações do sistema ou nos níveis de permissão de usuários deve ser registrada para garantir a rastreabilidade de ações que possam comprometer a segurança.

Acessos a dados sensíveis: Registros de acessos a informações confidenciais, como dados financeiros ou pessoais, são essenciais para identificar possíveis violações de privacidade ou abuso de privilégios.