UC- SISTEMAS COMPUTACIONAIS E SEGURANÇA

Maria Eduarda Medeiro Porto 824144948

ORIENTADOR: Robson Calvetti

PRÁTICA 07- ANÁLISE DE RISCOS

ATIVIDADE 1- Resolução dos exercícios de revisão

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

Pentest = teste de penetração. É um método de avaliação de segurança que simula um ataque cibernético contra um sistema de computador ou rede para avaliar suas vulnerabilidades e identificar brechas de segurança. O objetivo é identificar vulnerabilidades e recomendar medidas para remediar essas vulnerabilidades e proteger o sistema contra ataques mal-intencionados. As etapas de um pentest são:

1. Planejamento e preparação: Identificação dos objetivos e limites do teste

2. Reconhecimento: Coleta de informações públicas sobre o sistema ou rede e Identificação de possíveis vulnerabilidades e pontos de entrada

3. Varredura: Uso de ferramentas de varredura para identificar vulnerabilidades e serviços em execução e Identificação de possíveis pontos de entrada e vulnerabilidades

4. Vulnerabilidade: Identificação de vulnerabilidades específicas e sua exploração e Uso de técnicas de ataque para explorar vulnerabilidades

5. Exploitação: Uso de vulnerabilidades identificadas para obter acesso ao sistema ou rede e Coleta de informações confidenciais ou sensíveis

6. Post-exploitação: Análise das informações coletadas durante a exploração e Identificação de possíveis rotas de ataque adicionais

7. Relatório e remediação: Criação de um relatório detalhado sobre as vulnerabilidades identificadas e recomendações para remediar essas vulnerabilidades e Implementação de medidas para remediar as vulnerabilidades identificadas.

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

- Ataque de Negação de Serviço (DoS)- visa sobrecarregar um sistema ou rede com tráfego de rede fake, tornando-o indisponível para os usuários legítimos. Isso é feito enviando uma grande quantidade de pacotes de dados para o sistema, consumindo recursos e tornando-o incapaz de responder às solicitações legítimas.

-Ataque de Negação de Serviço Distribuído (DDoS)- é uma variante do ataque DoS, mas envolve múltiplos dispositivos (geralmente botnets) enviando tráfego de rede fake para o sistema. Isso torna o ataque mais difícil de bloquear e mais eficaz em sobrecarregar o sistema.

-Ramsonware- é um tipo de malware que criptografa os arquivos, dispositivos ou sistemas de uma vítima, tornando-os inacessíveis e inutilizáveis até que um resgate seja pago ao atacante. Isso geralmente é feito criptografando os dados e adicionando extensões aos arquivos criptografados.

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)?

O conceito se refere a: “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.

RECURSO	FUNCIONAMENTO	AÇÃO	RESPOSTA
FIREWALL	Bloqueia ou permite o tráfego de rede de entrada ou saída com base em regras de segurança pré-definidas	Bloqueia o tráfego baseado nas regras pré definidas	Bloqueia ou permite o tráfego
IDS	Monitora o tráfego de rede em busca de sinais de acesso não autorizado ou atividade maliciosa	Bloqueia o tráfego suspeito	Alerta os adm
IPS	Monitora o tráfego de rede em busca de sinais de acesso não autorizado ou atividade maliciosa e toma medidas para evitá-lo	Gera alertas para o adm quando detecta anomalias	Bloqueia ou elimina o tráfego malicioso

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.

Use senhas fortes que contenham letras, números e símbolos, mas que não seja tão grande; utilize a autenticação de dois fatores; use um gerenciador de senhas e evite usar senhas com dados que possam ser encontrados facilmente na internet

6) Observe a imagem a seguir.
Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade- A vulnerabilidade é o uso do sistema operacional falsificado, que não pode ser configurado corretamente e não irá receber as devidas atualizações.

b) A ameaça- Um baixo funcionamento adequado e risco de infecção de vírus e malwares.

c) Uma ação defensiva para mitigar a ameaça- Substituir o sistema falsificado por um original licenciado.

7) Observe a imagem a seguir.
Do ponto de vista da segurança da informação, identifique:
a) A vulnerabilidade- O uso de uma credencial de usuário muito fraca

b) A ameaça- Facilidade de ser quebrado por um indivíduo mal intencionado que poderá acessar o sistema.

c) Uma ação defensiva para mitigar a ameaça- Trocar as credenciais de acesso para outras que sejam mais seguras e de conhecimento do adm da rede.

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;
Deve cifrar com a chave pública do Bob

b) como Bob deverá decifrar a mensagem de Ana corretamente;
Deve decifrar com a sua chave privada

c) como Ana deverá cifrar a mensagem antes de enviar para Carlos;
Deve cifrar com a sua chave privada

d) como Carlos deverá decifrar a mensagem de Ana corretamente.
Deve decifrar com a chave pública da 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.

A CA gera um resumo dos dados de identificação do Banco através de uma função HASH. O resultado da função será criptografada com a chave privada de origem (Banco), assim obtém-se a assinatura digital. Para a validação da assinatura digital, o cliente do banco deve decifrar-la com a chave pública do emissor, contida no certificado. Em seguida, o HASH deverá ser calculado sobre a mensagem enviada. Se o valor calculado coincidir com o valor do HASH decifrado (a partir da assinatura digital), a mensagem é então validada.

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

Integridade: garantia de que as mensagens recebidas do Banco não sofreram alterações
Autenticação da origem: garantia de que as mensagens vêm da origem correta
Não repúdio: o banco não pode negar as mensagens

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.

-Acesso de arquivos realizados
-uso de privilégios
-endereços e protocolos de redes usados
-transações realizadas pelos usuários