Praatica07

Exercícios de Revisão

1) Um Pentest (teste de penetração) é uma simulação controlada de um ataque cibernético a um sistema, rede ou aplicativo, com o objetivo de identificar vulnerabilidades que um invasor poderia explorar.

As etapas de um Pentest são: Varredura, exploração, escalação de privilégios e ocultação

2) 1. Ataques DDoS: Os ataques DDoS envolvem a sobrecarga de um servidor, serviço ou rede com um tráfego excessivo, proveniente de várias fontes (geralmente uma botnet).

2. Ransomware: O ransomware é um tipo de malware que criptografa os arquivos do sistema e exige um resgate para a chave de descriptografia.

3. TCP SYN Flood: é um tipo de ataque de negação de serviço (DoS) que visa comprometer a disponibilidade de um servidor ou serviço.

3)Conformidade

4) Função Principal:

Firewall (Controlar o tráfego de entrada e saída com base em regras de segurança.)

IDS (Monitorar o tráfego de rede e detectar atividades suspeitas ou não autorizadas.)

IPS (Monitorar e responder em tempo real a atividades maliciosas, bloqueando ou prevenindo ações indesejadas.)

Tipo de Ação:

Firewall (Permitir ou bloquear tráfego com base em regras predefinidas.)

IDS (Alerta e notifica administradores sobre potenciais intrusões, mas não bloqueia.)

IPS (Bloqueia automaticamente o tráfego suspeito e previne a exploração de vulnerabilidades.)

Localização:

Firewall (Geralmente colocado na borda da rede, entre a rede interna e externa.)

IDS (Pode ser implementado em diferentes pontos da rede (borda ou interna).)

IPS (Similar ao IDS, pode ser implementado na borda ou em pontos críticos da rede.)

Resposta a Ameaças:

Firewall (Não responde ativamente a ameaças; apenas controla o tráfego.)

IDS (Apenas relata eventos suspeitos, sem ação corretiva.)

IPS (Responde ativamente, bloqueando o tráfego malicioso em tempo real.)

5) Não usar a mesma senha para todas as coisas, usar senhas longas e seguras sem usar senhas com dados que possam ser conseguidos facilmente) e não clicar em links estranhos recebidos pela internet.

6)

A) Vulnerabilidade: Uso de sistema operacional falsificado (Sistema operacional falso instalado, fazendo com que não receba atualizações).

B) A ameaça: Instabilidade, baixo desempenho e possibilidade de infecção por malware.

C) Uma ação defensiva para mitigar a ameaça: Desinstalar as copias falsificadas e instalar as copias legítimas.

7)

A) Vulnerabilidade: Credenciais fracas por usar nome de usuário padrão.

B) A ameaça: Por ser credenciais fracas um cracker terá maior facilidade em invadir.

C) Uma ação defensiva para mitigar a ameaça: Renomear todos os usuários com privilégios de administração n rede.

8)

a) como Ana deverá cifrar a mensagem antes de enviar para Bob: Com a chave pública de Bob

b) como Bob deverá decifrar a mensagem de Ana corretamente: Com a sua chave Privada.

d) como Ana deverá cifrar a mensagem antes de enviar para Carlos: Com a sua chave Privada.

e) como Carlos deverá decifrar a mensagem de Ana corretamente: Com a chave pública de Ana.

9) A CA Serctigo gera um resumo dos dados de identificação do Banco através de uma função HASH. O resultado da função HASH será criptografado com a chave privada da origem (Banco), assim obtém-se a assinatura digital. Para a validação da assinatura digital, o cliente do banco deve decifrá-la com a chave pública do emissor, contida no certificado. Em seguida, o HASH deve 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.

b) Autenticação da origem: garantia de que as mensagens realmente vêm da origem especificada no certificado, no caso o Banco do Brasil. Integridade: garantia de que as mensagens recebidas do Banco do Brasil estão íntegras, e não sofreram nenhuma alteração acidental ou intencional. Pode, ainda, ser citado o não-repúdio – a garantia de que a origem (o Banco) não pode repudiar, ou refutar as mensagens por ele enviadas.

10) Registro de tentativas de acesso ao sistema, Id (identificação dos usuários) e arquivos acessados e o tipo do acesso.