Questões

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

R: Pentest uma prática que envolve testar a segurança de projeto desenvolvido da simulação de um ataque. O objetivo é identificar vulnerabilidades que podem ser exploradas por hackers ou malwares, permitindo que os administradores corrijam esses pontos fracos antes que possam ser explorados de forma maliciosa. Esse teste é dividido em 4 etapas que são varredura, exploração, escalação de privilégios e ocultação.

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

R. São exemplos de ataques cibernéticos que podem comprometer a disponibilidade de sistema o ataque de Negação de Serviço, onde um único atacante sobrecarrega um servidor com solicitações falsas, esgotando seus recursos e com isso faz servidor ser incapaz de atender usuários legítimos, resultando em indisponibilidade temporária do serviço. Outra forma é o ataque Distribuído de Negação de Serviços, no qual dispositivos atacam simultaneamente um servidor com um grande volume de tráfego e torna o sistema indisponível para usuários legítimos e o terceiro é o Ransomware que criptografa dados ou bloqueia o acesso a um sistema até que um resgate seja pago e isso bloqueia o acesso a dados essenciais, causando a paralisação de operações e a indisponibilidade do sistema até que o problema seja resolvido.

1. 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)?

A palavra é Conformidade.

1. 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 | Características |
| **Firewall** | * Filtra o tráfego de rede com base em regras predefinidas para permitir ou bloquear pacotes. * Opera no nível de rede e/ou transporte, analisando pacotes e suas características. * Permite ou nega o tráfego com base em políticas de segurança. * Pode ser baseado em estado (stateful) ou em pacotes (stateless). * Normalmente, é colocado na borda da rede (entre a rede interna e externa). * Requer atualização regular de regras e políticas. |
| **IDS (Intrusion Detection System)** | * Monitora o tráfego de rede para detectar atividades suspeitas ou não autorizadas. * Analisando o tráfego e gerando alertas quando detecta comportamentos anômalos. * Gera alertas para administradores, mas não interfere no tráfego. * Pode ser baseado em assinatura (detecção de padrões conhecidos) ou anômala (detecção de comportamentos incomuns). * Pode ser implementado em diversos pontos da rede, como em hosts ou na borda. * Necessita de análise e resposta a alertas para ajustar regras de detecção. |
| **IPS (Intrusion Prevention System)** | * Monitora e bloqueia ativamente o tráfego malicioso em tempo real. * Similar ao IDS, mas com a capacidade de bloquear o tráfego malicioso assim que é identificado. * Bloqueia automaticamente pacotes maliciosos, além de gerar alertas. * Pode ser baseado em assinatura e anômala, mas prioriza a prevenção em tempo real. * Geralmente colocado em linha com o tráfego (entre a fonte e o destino) para interceptar pacotes. * Também requer manutenção de regras e pode necessitar de ajustes constantes para minimizar falsos positivos. |

Parte superior do formulário

Parte inferior do formulário

1. 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. Não repetir a mesma senha em vários sistemas, usar um gerenciador de senhas, usar senhas de cunho não pessoal.

1. Observe a imagem a seguir. Do ponto de vista da segurança da informação, identifique:
2. A vulnerabilidade: Utilização de sistema falsificado.
3. A ameaça: Instabilidade
4. Uma ação defensiva para mitigar a ameaça: Instalação do programa original.
5. Observe a imagem a seguir. Do ponto de vista da segurança da informação, identifique:
6. A vulnerabilidade: Usuário administrador muito padrão
7. A ameaça: Fácil identificação da credencial
8. Uma ação defensiva para mitigar a ameaça: Mudar as credenciais para algo mais complexo
9. 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:
   1. como Ana deverá cifrar a mensagem antes de enviar para Bob;

Chave pública de Bob.

* 1. como Bob deverá decifrar a mensagem de Ana corretamente;

Chave privada.

* 1. como Ana deverá cifrar a mensagem antes de enviar para Carlos;

Chave privada.

* 1. como Carlos deverá decifrar a mensagem de Ana corretamente.

Chave pública de Ana.

1. Observe as imagens a seguir: As imagens apresentam informações do certificado digital do site www.bb.com.br. Com base nelas, responda:

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 utilização de certificados digitais e chaves criptográficas no Banco do Brasil garante a segurança das comunicações entre clientes e servidores. O cliente confirma sua identidade usando um certificado digital e criptografa dados com a chave pública do servidor. O servidor apresenta seu certificado para validação pelo cliente e utiliza sua chave privada para descriptografar as informações recebidas. O banco emprega chaves públicas e privadas para proteger dados sensíveis, autenticar usuários e garantir a integridade e autenticidade das transações por meio de assinaturas digitais, promovendo assim comunicações seguras e protegidas contra fraudes.

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

Autenticação e Identidade e Segurança dos Dados pessoais

1. 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.

Registros de Login e Logout

Registros de Atividades de Acesso a Dados Sensíveis

Registros de Erros e Exceções