Pedro Paulo Alves dos Santos - 823217810

1) Penetration Test (Pentest) e Suas Fases

O Pentest (ou Teste de Penetração) é uma metodologia de segurança destinada a avaliar a robustez de sistemas de software ou hardware. O processo envolve testadores que tentam ativamente explorar vulnerabilidades para verificar a possibilidade de comprometer aplicativos, dados ou recursos do ambiente. O Pentest é, essencialmente, uma simulação controlada de um ataque real.

As fases típicas de um pentest são:

- Varredura
- Exploração
- Escalação de privilégios
- Ocultação

2) Ataques que Afetam Diretamente a Disponibilidade de Sistemas

Três exemplos de ataques que comprometem diretamente a disponibilidade de sistemas são:

1. Ataques de Negação de Serviço (DoS/DDoS): Sobrecarregam os recursos do sistema ou da rede com tráfego excessivo, impedindo que usuários legítimos acessem o serviço. O DDoS utiliza múltiplas fontes para potencializar o ataque.

2. Ataques TCP (SYN Flood/TCP ACK Attack): Explorando o protocolo TCP, esses ataques visam esgotar a capacidade de conexões do servidor, mantendo um grande número de conexões incompletas abertas.

3. Ransomware: Este tipo de malware compromete a disponibilidade ao criptografar ou bloquear o acesso ao sistema, exigindo um resgate para a restauração.

3) O Conceito de Segurança da Informação Relacionado à Legislação

O conceito que estabelece a obrigação de uma empresa em observar a legislação, regulamentos internos e obrigações contratuais na implementação dos seus requisitos de segurança é a **conformidade.**

4) Comparativo entre Firewall, IPS e IDS

Parâmetro	FIREWALL	IPS (Sistema de Prevenção de Intrusão)	IDS (Sistema de Detecção de Intrusão)
Filosofia/Função	Filtra o tráfego de rede (entrada/saída) com base em um conjunto de regras predefinidas.	Inspeciona, detecta e **impede proativamente** tráfego malicioso e ataques.	**Monitora** o tráfego em busca de atividades ou violações de política e **gera alertas**.
Princípio de Ação	Realiza a filtragem primariamente com base em endereços **IP e números de porta**.	Inspeciona o tráfego **em tempo real** em busca de padrões ou assinaturas de ataque e o **bloqueia**.	Monitora o tráfego **em tempo real** em busca de padrões ou assinaturas de ataque para **alertar**.
Posicionamento na Rede	Deve ser a primeira linha de defesa, na borda da rede.	Deve ser instalado após o Firewall na rede.	Deve ser colocado após o firewall.
Ação Primária	Bloqueia o tráfego de acordo com as regras configuradas.	Bloqueia o tráfego suspeito.	Gera alarmes/alertas.
Detecção de Ataques Zero Day	Não, pois filtra pacotes com base em regras conhecidas.	Sim, pois utiliza prevenção baseada em anomalias.	Sim, pois utiliza detecção baseada em anomalias.

5) Recomendações para Proteger Senhas

Três conselhos essenciais para a proteção de senhas são:

1. Criação de Credenciais Robustas: Utilizar senhas com números aleatórios com muitos dígitos, além de caracteres especiais, letras maiúsculas e minúsculas. Deve-se evitar informações pessoais ou padrões previsíveis.

2. Uso de Gerenciamento e Antirrepetição: Não reutilizar a mesma senha em sistemas diferentes. Recomenda-se a utilização de um gerenciador de senhas.

3. Implementação de Autenticação Multifator (MFA): Sempre que possível, utilizar a autenticação de múltiplos fatores para adicionar uma camada de segurança.

6) Análise de Segurança: Sistema Operacional Falsificado

- a) A Vulnerabilidade: Sistema operacional falsificado instalado. O sistema não recebe atualizações de segurança importantes.
- b) A Ameaça: Aumento do risco de infecção por malware e instabilidade do sistema a longo prazo.
- c) Ação Defensiva (Mitigação): Remoção da cópia não licenciada, instalando cópias legítimas ou optando por um sistema operacional open source.

7) Análise de Segurança: Credenciais Padrão (Admin)

A imagem de configuração do Apache Tomcat Server mostra o nome de usuário administrador preenchido com "admin".

- a) A Vulnerabilidade: Uso de credenciais fracas para usuário administrador. "Admin" é um nome de usuário padrão conhecido em muitos serviços.
- b) A Ameaça: O invasor (cracker) terá mais facilidade para quebrar as credenciais e invadir o sistema.
- c) Ação Defensiva (Mitigação): Renomear todos os usuários com privilégios de administração na rede, evitando nomes de usuário padrão.

8) Criptografia Assimétrica para Confidencialidade e Autenticidade

Considerando a criptografia assimétrica, o uso das chaves deve ser o seguinte:

Cenário Bob (Objetivo: Sigilo/Confidencialidade)

- a) Cifragem por Ana: Ana deve cifrar a mensagem com a chave pública de Bob.
- b) Decifragem por Bob: Bob deve decifrar a mensagem com a sua chave privada.

Cenário Carlos (Objetivo: Autenticidade/Garantia da Origem)

- a) Cifragem (Assinatura) por Ana: Ana deve cifrar a mensagem com a sua chave privada.
- b) Decifragem (Verificação) por Carlos: Carlos deve decifrar/verificar a assinatura com a chave pública de Ana.

9) Análise do Certificado Digital do Banco do Brasil

9.a) Uso das Chaves na Origem e Destino

O certificado é utilizado para estabelecer a confiança e a integridade:

- Na Origem (Banco): A Autoridade Certificadora (CA) gera um resumo (HASH) dos dados do Banco. Esse HASH é criptografado com a chave privada da origem para criar a assinatura digital.
- No Destino (Cliente): O cliente decifra a assinatura digital usando a chave pública do emissor. Em seguida, o HASH deve ser calculado sobre a mensagem recebida. A validação ocorre se o HASH calculado coincidir com o HASH decifrado.

9.b) Benefícios de Segurança do Certificado Digital

A utilização de um certificado digital oferece benefícios de segurança para transações eletrônicas, como:

1. Autenticação da Origem: Garante que as mensagens são provenientes da origem especificada no certificado (o Banco do Brasil).
2. Integridade: Assegura que o conteúdo das mensagens não foi alterado durante a transmissão.
3. Não-Repúdio: Impede que a origem (o Banco) negue ter enviado as mensagens ou realizado a transação.

10) Registros de Atividades de Usuários para Auditoria

A norma ISO 27002 exige que registros (log) de eventos e atividades dos usuários sejam gerados e analisados regularmente para fins de segurança.

Três registros de atividade cruciais para auditoria de segurança são:

1. Identificação do Usuário: O registro do ID dos usuários.
2. Eventos-Chave de Acesso: O registro de datas, horários e detalhes de eventos-chave, como o horário de entrada (log-on) e saída (log-off) no sistema.
3. Tentativas de Acesso Registradas: O registro das tentativas de acesso ao sistema, sejam elas aceitas ou rejeitadas.