Exercícios revisão

Arthur Silva Carvalho

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

Pentest (ou teste de penetração) é um processo de simulação de ataques a sistemas computacionais com o objetivo de identificar vulnerabilidades e falhas de segurança antes que sejam exploradas por atacantes maliciosos.

Etapas de um pentest:

- Planejamento e Reconhecimento: definição do escopo, coleta de informações sobre o alvo.
- Varredura: identificação de portas abertas, serviços e sistemas operacionais.
- Ganho de Acesso: tentativa de explorar vulnerabilidades para invadir o sistema.
- Manutenção de Acesso: simula persistência do invasor dentro do sistema.
- Análise e Relatório: documentação de todas as descobertas, falhas e recomendações de correção.

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

- Ataque DDoS (Distributed Denial of Service): sobrecarrega um servidor ou rede com múltiplas requisições simultâneas, deixando o serviço fora do ar.
- Ransomware: malware que criptografa dados do sistema e exige pagamento para liberação, podendo tornar o sistema inutilizável.
- Sabotagem de hardware: ataques físicos ou lógicos que danificam equipamentos ou sistemas, resultando em indisponibilidade dos serviços.

3) Qual conceito está sendo descrito no texto?
Conformidade.

4) Comparação entre Firewall, IDS e IPS

Na segurança de redes, firewalls, IDS (Intrusion Detection System) e IPS (Intrusion Prevention System) são recursos fundamentais, cada um com sua função específica:

- Firewall: Atua como uma barreira de controle de tráfego entre redes. Ele permite ou bloqueia conexões com base em regras predefinidas, como endereços IP, portas e protocolos. Seu principal objetivo é filtrar o tráfego de entrada e saída, impedindo acessos não autorizados.
- IDS (Sistema de Detecção de Intrusão): Tem a função de monitorar o tráfego da rede ou de um sistema para detectar atividades suspeitas ou maliciosas. O IDS não interfere diretamente no tráfego, apenas gera alertas para que administradores tomem providências. Ele é útil para identificar tentativas de ataque ou violações de políticas.
- IPS (Sistema de Prevenção de Intrusão): Vai além do IDS, pois além de monitorar e detectar, o IPS atua automaticamente, podendo bloquear tráfego malicioso em tempo real. Ele pode encerrar sessões, descartar pacotes ou até reconfigurar firewalls ao detectar uma ameaça.

5) Três conselhos para proteger senhas:

- Use senhas fortes e únicas, combinando letras maiúsculas, minúsculas, números e símbolos.
- Ative a autenticação em dois fatores (2FA) sempre que possível.
- Evite reutilizar senhas em diferentes serviços e utilize um gerenciador de senhas para armazená-las com segurança.

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

a) A vulnerabilidade:
Uso de sistema operacional pirata ou não licenciado, que pode não receber atualizações de segurança e estar mais exposto a falhas conhecidas.

b) A ameaça:
Possibilidade de exploração por malware, hackers ou softwares maliciosos, aproveitando a ausência de atualizações ou backdoors presentes em versões falsificadas.

c) Uma ação defensiva para mitigar a ameaça:
Utilizar uma cópia legítima e licenciada do sistema operacional, garantindo acesso a atualizações de segurança, suporte oficial e integridade do sistema.

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

a) A vulnerabilidade:
Uso de credenciais administrativas padrão ou fracas (ex: "admin" como nome de usuário) durante a instalação de um serviço crítico.

b) A ameaça:
Ataques de força bruta, dicionário ou acesso não autorizado ao painel de administração do Tomcat, possibilitando controle total do servidor por um invasor.

c) Uma ação defensiva para mitigar a ameaça:

- Alterar o nome de usuário e usar uma senha forte e complexa.
- Restringir o acesso ao painel de administração por IP.
- Implementar autenticação multifator (MFA), se possível.

8)

a) Como Ana deverá cifrar a mensagem antes de enviar para Bob:

Bob quer sigilo, ou seja, apenas ele deve conseguir ler a mensagem.

Ana deve cifrar a mensagem com a chave pública de Bob.
Assim, só Bob conseguirá decifrá-la usando sua chave privada.

b) Como Bob deverá decifrar a mensagem de Ana corretamente:

Bob deverá usar sua chave privada para decifrar a mensagem que Ana cifrou com sua chave pública.

c) Como Ana deverá cifrar a mensagem antes de enviar para Carlos:

Carlos quer autenticidade, ou seja, certeza de que foi Ana quem enviou.

Ana deve cifrar a mensagem com sua própria chave privada.
Assim, qualquer pessoa (inclusive Carlos) poderá decifrar com a chave pública dela, provando que veio de Ana.

d) Como Carlos deverá decifrar a mensagem de Ana corretamente:

Carlos deverá usar a chave pública de Ana para decifrar a mensagem.
Se conseguir, ele confirma que foi Ana quem enviou, já que só a chave privada dela poderia ter cifrado.

9)

9.a) Utilização do certificado e chaves criptográficas:

O certificado digital do Banco do Brasil garante a identidade do servidor e permite uma comunicação segura.

- O servidor apresenta o certificado com sua chave pública, validado por uma autoridade confiável.
- O navegador do usuário usa essa chave pública para verificar a autenticidade e negociar uma conexão segura.
- A chave pública garante a autenticidade do banco.
- A chave privada é usada pelo banco para decifrar ou assinar dados durante a conexão.

9.b) Benefícios de segurança do certificado digital:

1. Autenticidade – Confirma que o site é realmente do Banco do Brasil.
2. Confidencialidade e integridade – Protege os dados trocados contra leitura ou alteração por terceiros.

10)

1. Tentativas de login (bem-sucedidas e falhas):

Permite identificar acessos legítimos e tentativas suspeitas (como brute force ou tentativas de invasão).

2. Acessos a dados sensíveis ou sistemas críticos:

Registro de quando, por quem e de onde dados importantes (ex: dados financeiros, de clientes ou sistemas administrativos) foram acessados.

3. Alterações em configurações do sistema ou permissões de usuários:

Controla mudanças que podem impactar a segurança ou a integridade do ambiente — como um usuário sendo promovido a administrador sem justificativa.