

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

R: Pentest (Penetration Test) é um teste de penetração utilizado para identificar vulnerabilidades em sistemas, redes ou aplicativos, explorando-as como um atacante faria.

Etapas de um pentest:

- Planejamento e reconhecimento: Entendimento do escopo e coleta de informações sobre o alvo.
- Varredura: Utilização de ferramentas para identificar vulnerabilidades e entender como o alvo responde a ataques.
- Obtenção de acesso: Tentativa de explorar as vulnerabilidades descobertas.
- Manutenção do acesso: Verificar se o acesso pode ser mantido para ataques futuros.
- Relatório: Documentar os resultados, vulnerabilidades descobertas e recomendações de mitigação.

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

- DDoS (Distributed Denial of Service): Inunda o sistema com tráfego excessivo, fazendo com que ele se torne indisponível.
- Ransomware: O software malicioso criptografa arquivos e torna o sistema inutilizável até que um resgate seja pago.
- Ataque de Exaustão de Recursos: Consome os recursos de um sistema (como CPU ou memória) através de solicitações repetitivas ou maliciosas, causando falha ou lentidão.

3. Conceito relacionado ao cumprimento de requisitos de segurança, regulamentos internos e acordos internacionais (em uma palavra)?

R: Conformidade.

4. Comparação entre firewalls, IDS e IPS:

- Firewall: Monitora e controla o tráfego de rede, atuando como uma barreira entre redes confiáveis e não confiáveis.
- IDS (Intrusion Detection System): Sistema de detecção de intrusões que monitora atividades suspeitas e gera alertas, mas não toma ações corretivas.
- IPS (Intrusion Prevention System): Sistema de prevenção de intrusões que não apenas detecta atividades suspeitas, mas também bloqueia ações maliciosas automaticamente.

5. Três conselhos para proteger senhas:

R: Use senhas longas e complexas, combinando letras, números e caracteres especiais. Ative a autenticação de dois fatores (2FA) sempre que possível. Utilize um gerenciador de senhas para armazenar suas credenciais com segurança.

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

R: Vulnerabilidade: Qualquer falha ou fraqueza em um sistema que pode ser explorada.

Ameaça: O possível risco ou agente que pode explorar a vulnerabilidade (por exemplo, um invasor).

Ação defensiva: Implementar patches de segurança, firewalls, ou monitoramento contínuo para mitigar a ameaça.

7. Ana deseja criptografar mensagens para Bob e Carlos.

Como deve fazer?

Para Bob:

R: Cifrar para Bob: Ana deve usar a chave pública de Bob para criptografar a mensagem.

Decifrar por Bob: Bob deve usar sua chave privada para decifrar a mensagem.

Para Carlos:

Cifrar para Carlos: Ana deve assinar digitalmente a mensagem usando sua chave privada, provando a autenticidade.

Decifrar por Carlos: Carlos usará a chave pública de Ana para verificar a assinatura e garantir que a mensagem é legítima.

8. Utilização do certificado digital do Banco do Brasil (www.bb.com.br):

9. A) O certificado digital é utilizado para garantir a autenticação entre o cliente e o servidor, criptografando as informações trocadas. O Banco do Brasil utiliza sua chave privada para criar assinaturas digitais, enquanto os usuários utilizam a chave pública para verificar a autenticidade e garantir a integridade dos dados.

9. B) Benefícios de segurança:

Confidencialidade: As informações trocadas são criptografadas, protegendo contra a interceptação.

Autenticidade: Garante que o site é legítimo e que as informações vêm de uma fonte confiável.

10. Três registros importantes para auditoria de segurança (conforme ISO 27002:2013):

R: Registros de login/logout dos usuários.

Registros de acessos a dados confidenciais.

Registros de tentativas de falhas ou acessos não autorizados.