Carlos Eduardo Santos Gimenes RA:825154398

1) O que é um pentest? Quais são suas etapas?

Um pentest (teste de penetração) é uma simulação autorizada de ataque cibernético. Seu objetivo é detectar vulnerabilidades nos sistemas antes que sejam exploradas por agentes maliciosos.

As fases são:

* Planejamento - definição do escopo, metas e obtenção de autorização.
* Reconhecimento - coleta de informações públicas sobre o alvo.
* Varredura e enumeração - identificação de portas abertas, serviços ativos e possíveis pontosfrágeis.
* Exploração - tentativa de invasão com base nas vulnerabilidades descobertas.
* Pós-exploração - verificação de até onde o invasor poderia chegar (acesso a dados,escalonamento de privilégios).
* Relatório - documentação técnica dos achados, evidências e sugestões de correção.
* Reteste (opcional) - nova avaliação após correções feitas.

2) Descreva três tipos de ataque cibernético que afetam a disponibilidade de sistemas.

* Ataques DoS/DDoS: sobrecarregam sistemas com tráfego excessivo, esgotando recursos comobanda, CPU ou memória.
* Ransomware: bloqueia o acesso aos dados por criptografia, tornando o sistema inutilizável até opagamento de resgate.
* Ataques ao DNS: envenenamento ou sobrecarga de servidores DNS, impedindo que usuáriosacessem serviços pela rede.

1. Qual conceito da segurança da informação está relacionado ao cumprimento de leis e normas?

Compliance - refere-se à conformidade com leis, normas internas, contratos e acordos.

1. Compare as funções de firewall, IDS e IPS.

* Firewall: atua como uma barreira que permite ou bloqueia tráfego conforme regras configuradas.
* IDS (Sistema de Detecção de Intrusos): monitora a rede, detecta padrões suspeitos e gera alertas.- IPS (Sistema de Prevenção de Intrusos): semelhante ao IDS, mas também age para bloquear ameaças automaticamente.

5) Dê três recomendações para proteger senhas:

* Utilize um gerenciador de senhas para criar e armazenar combinações fortes e únicas.
* Ative autenticação multifator (MFA) sempre que possível.
* Nunca repita senhas entre diferentes serviços.

6) Sobre o uso de software pirata:

1. Vulnerabilidade: presença de software não licenciado na organização.
2. Ameaça: risco de malwares embutidos nos instaladores.
3. Mitigação: só utilizar software original, fazer varreduras regulares e promover conscientizaçãodos usuários.

7) Sobre sistemas sem controle de acesso:

1. Vulnerabilidade: ausência de autenticação obrigatória.
2. Ameaça: acesso não autorizado a informações.
3. Mitigação: implementação de cadastro e autenticação obrigatória para todos os usuários.

8) Como enviar mensagens seguras usando criptografia assimétrica:

1. Para garantir sigilo, Ana deve cifrar a mensagem usando a chave pública de Bob.
2. Bob decifra a mensagem com sua chave privada.
3. Para garantir autenticidade, Ana deve assinar a mensagem com sua chave privada.
4. Carlos verifica a assinatura com a chave pública de Ana.

9) Sobre certificados digitais no site www.bb.com.br:

1. O servidor do banco guarda a chave privada. O cliente valida o certificado e envia um segredocifrado com a chave pública do banco.
2. Benefícios:

* Autenticidade do site, evitando fraudes.
* Criptografia do tráfego, protegendo a integridade e confidencialidade da informação.

10) Três registros relevantes para auditoria de segurança:

* Log de login/logout (data, hora, IP, sucesso/erro).
* Acesso a arquivos ou sistemas sensíveis.
* Tentativas de ações com privilégios elevados.Estudo de Caso 1: Segurança no Acesso Remoto

1. O site tinha criptografia ativa?

Sim. O ícone de segurança mostra uso de HTTPS (SSL/TLS), protegendo os dados durante a transmissão.

1. Como melhorar a segurança no acesso remoto?

* Adotar autenticação multifator.
* Proibir compartilhamento de senhas por voz ou texto.
* Usar certificados digitais para autenticação.
* Monitorar acessos e configurar alertas.Estudo de Caso 2: Uso Indevido da Internet 1) A política de uso da web é severa?

É restrita, mas visa proteger os ativos da empresa. Seria útil prever exceções em horários livres.

1. Ron estava justificado?

Ele agiu por impulso após meses de esforço, mas violou conscientemente a política da empresa.

1. Qual atitude o gerente Andy deve tomar?

Dialogar com Ron, considerar o histórico positivo dele e negociar a reativação de acesso. Sugerir ajustes na política para pequenos usos recreativos controlados.