Atividades – Aula 07: Exercícios de Revisão e Estudos de Caso

Aluno: Joao Victor de Souza Moreira

RA: 825135230

Curso: Análise e Desenvolvimento de Sistemas

Disciplina: Sistemas Computacionais e Segurança

Professor: Calvetti

Parte 1 – Exercícios de Revisão

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

Pentest é um teste de invasão realizado para identificar vulnerabilidades em sistemas. As etapas são: planejamento, coleta de informações, exploração, pós-exploração e relatório final.

2) Explique o funcionamento de 3 ataques que comprometem a DISPONIBILIDADE de sistemas.

Ataques DoS/DDoS (sobrecarga de tráfego), ransomware (bloqueia acesso ao sistema) e sabotagem física (danos a servidores).

3) Conceito do texto (HINTZBERGEN, 2018).

Conformidade.

4) Quadro comparativo entre Firewall, IDS e IPS.

Firewall: filtra tráfego entre redes. IDS: detecta intrusões. IPS: detecta e bloqueia intrusões automaticamente.

5) Três conselhos para proteger senhas.

Usar senhas fortes, não reutilizar senhas e habilitar autenticação de dois fatores.

6) Imagem 1 – Identificação.

Vulnerabilidade: uso indevido de credenciais. Ameaça: acesso não autorizado. Ação defensiva: autenticação multifator.

7) Imagem 2 – Identificação.

Vulnerabilidade: ausência de antivírus ou atualização. Ameaça: malware. Ação defensiva: uso de antivírus atualizado.

8) Criptografia de mensagens (Ana, Bob e Carlos).

a) Para Bob: Ana cifra com a chave pública de Bob. b) Bob decifra com sua chave privada. c) Para Carlos: Ana assina com sua chave privada. d) Carlos valida com a chave pública de Ana.

9) Certificado digital do Banco do Brasil.

a) No envio, o site usa sua chave privada e o cliente usa a chave pública para validar. b) Benefícios: autenticação e integridade das transações.

10) Registros importantes para auditoria.

Logins, tentativas de acesso e modificações de arquivos.

Parte 2 – Estudo de Caso 1 – Criptografia e Firewalls

1) Sim. O firewall e o servidor Web oferecem criptografia TLS/SSL, que protege os dados durante a transmissão entre cliente e servidor.

2) O acesso poderia ser mais seguro com autenticação multifator, uso de VPN, e proibição de compartilhamento de senhas por voz ou mensagem.

Parte 3 – Estudo de Caso 2 – Servidores Proxy e Firewalls

1) A política da ATI é adequada, pois mantém a segurança e evita uso indevido da rede corporativa.

2) Não. Ron não estava justificado, pois desrespeitou as regras de uso da Internet da empresa.

3) Andy deve conversar com Ron, aplicar orientação educativa e garantir que ele compreenda as políticas de segurança, considerando seu histórico de bom funcionário.