Sistemas Computacionais e Segurança

Rafael Henrique Garbelini Alberto 825114430

Eduardo Barbosa Santos 825162647

Guilherme Germano Alves Cardoso 825165658

Gabriel Dassi Winiemcko 825149898

Arthur Cagnani Nicacio - 825140545

Atividade 1 – Resolução dos Exercícios de Revisão

São Paulo, Abril de 2025

---

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

O pentest (teste de intrusão) é uma simulação controlada de ataques reais a sistemas de informação, com o objetivo de identificar vulnerabilidades e avaliar a eficácia dos mecanismos de segurança existentes.

As principais etapas de um pentest são:

1. Planejamento e reconhecimento;
2. Varredura e enumeração;
3. Ganha de acesso;
4. Manutenção de acesso;
5. Análise e geração de relatório.

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

1. **DDoS (Distributed Denial of Service):** Envia um grande volume de tráfego para um sistema até que ele se torne indisponível.
2. **Buffer Overflow:** Explora falhas na alocação de memória para travar ou comprometer o sistema.
3. **Ransomware:** Bloqueia o acesso aos dados e sistemas até que um resgate seja pago, afetando diretamente a disponibilidade.

3. Qual é o conceito importante citado no fragmento de texto de Hintzbergen?

Compliance (Conformidade).

4. Quadro comparativo: Firewall, IDS e IPS

Recurso	Função Principal	Atuação Passiva	Atuação Ativa
Firewall	Filtragem de tráfego por regras	Sim	Sim
IDS (Intrusion Detection System)	Detecção de intrusão	Sim	Não
IPS (Intrusion Prevention System)	Prevenção de intrusão	Não	Sim

5. Três conselhos para proteger senhas:

1. Criar senhas fortes e únicas;
2. Usar autenticação de dois fatores (2FA);
3. Não reutilizar senhas e evitar anotá-las fisicamente.

6. Análise de vulnerabilidade, ameaça e defesa (Imagem 1)

a) Vulnerabilidade: Porta aberta ou sistema desprotegido.

b) Ameaça: Exploração por agentes maliciosos.

c) Ação defensiva: Uso de firewall, atualizações constantes e varredura de segurança.

7. Análise de vulnerabilidade, ameaça e defesa (Imagem 2)

a) Vulnerabilidade: Senha fraca ou visível.

b) Ameaça: Roubo de credenciais.

c) Ação defensiva: Uso de gerenciador de senhas e MFA.

8. Mensagens criptografadas para 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 cifra com sua chave privada.

d) Carlos verifica a autenticidade com a chave pública de Ana.

9. Certificado digital do site www.bb.com.br

9.a) O certificado é assinado com a chave privada do BB, e os navegadores verificam com a chave pública. Assim, assegura-se a autenticidade e estabelece-se uma conexão segura.

9.b) Benefícios: Criptografia dos dados (confidencialidade); Validação da identidade do servidor (autenticidade).

10. Três registros importantes para auditoria de segurança:

1. Log de autenticação (login/logout);
2. Acessos negados ou tentativas de acesso indevido;
3. Modificações em arquivos ou parâmetros de configuração.