SEGURANÇA EM REDES E COMPUTADORES | 21181

Período de Realização

Decorre de 03 de novembro a 17 de novembro de 2025

Data de Limite de Entrega

17 de novembro de 2025, até às 23:59 de Portugal Continental

Temática / Tema / Conteúdos

Neste trabalho, os alunos aplicarão os conceitos básicos de segurança de computadores e redes para analisar um exemplo de arquitetura de rede. Identificarão possíveis vulnerabilidades, sugerirão mecanismos de segurança apropriados e justificarão essas recomendações com base nos princípios de segurança de computadores. Além disso, implementarão uma solução criptográfica básica para a confidencialidade dos dados num cenário fornecido.

Objetivos

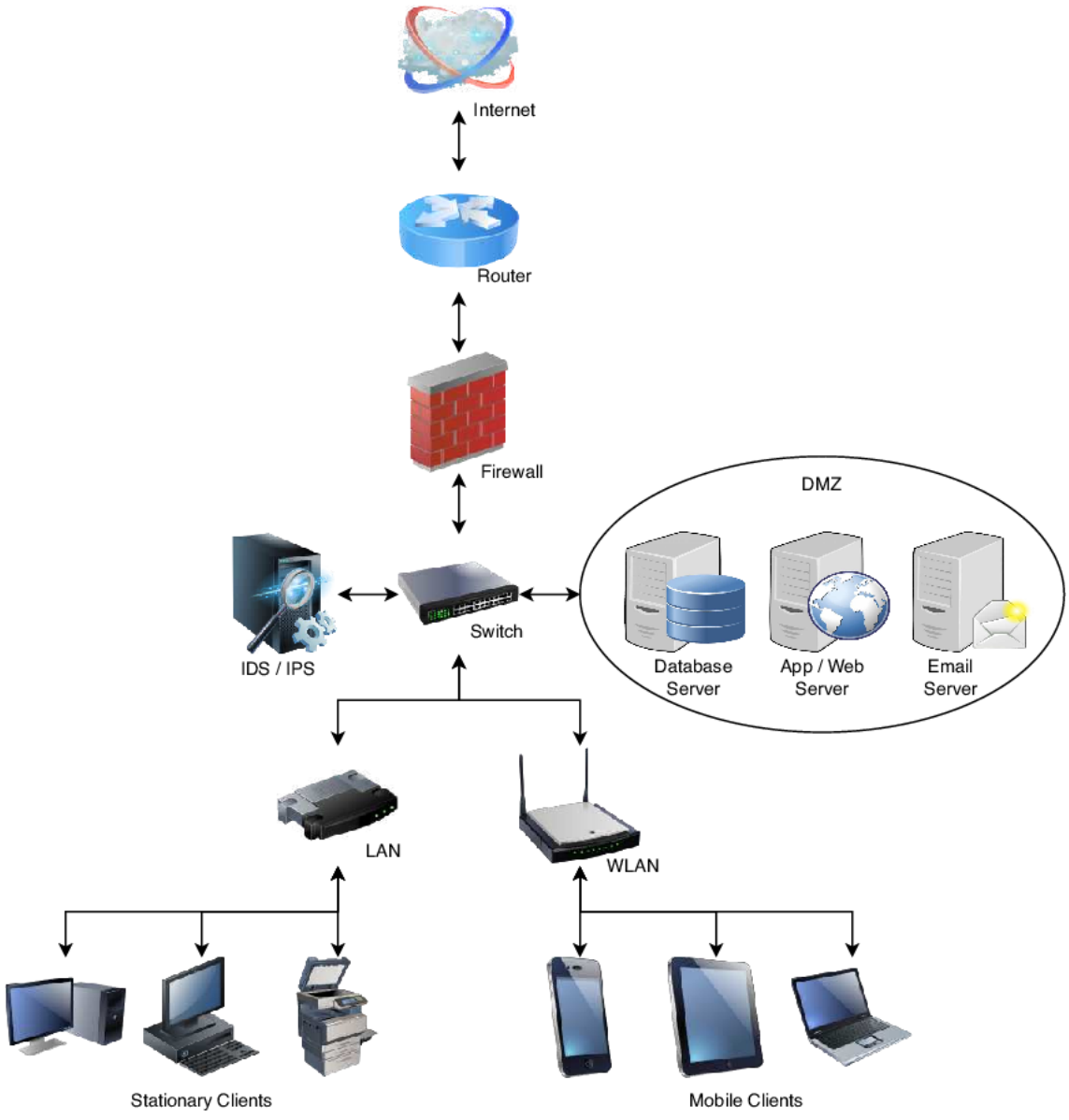
Os principais objetivos deste trabalho são:

- Aplicar os princípios de segurança de computadores a um cenário prático de segurança de rede.
- Identificar e analisar superfícies de ataque e ameaças.
- Propor e justificar controlos de segurança utilizando a confidencialidade, a integridade e a disponibilidade como princípios orientadores.

- Demonstrar uma compreensão da encriptação simétrica e assimétrica através da implementação de proteções criptográficas básicas.

Trabalho a desenvolver

Considere a seguinte arquitetura de rede simplificada, correspondendo a uma organização de média dimensão.



1. Análise de redes e ameaças

Considere o diagrama simplificado da arquitetura de rede que representa uma organização. Estude este diagrama cuidadosamente, identificando potenciais vulnerabilidades de segurança e superfícies de ataque.

Construa uma árvore de ataque com base em potenciais vetores de ameaça que visam diferentes partes da rede (por exemplo, servidores, pontos de acesso, ligações de rede).

Classifique cada ameaça identificada usando conceitos de segurança (confidencialidade, integridade, disponibilidade) e analise os possíveis tipos de ataque que podem explorar essas ameaças.

2. Estratégia de segurança e proposta de controlo

Com base na sua análise, sugira uma série de controlos de segurança concebidos para atenuar cada vulnerabilidade identificada. As suas recomendações devem considerar os princípios de segurança, incluindo o privilégio mínimo, a defesa em profundidade, a separação de privilégios e a segurança através da obscuridade.

Justifique as suas escolhas de controlo, explicando como reduzem especificamente o risco na rede, tendo em conta o custo, a viabilidade e o impacto na utilização do sistema.

3. Implementação da solução criptográfica

Desenvolva uma solução de encriptação simples para proteger os dados em trânsito na rede. É necessário implementar a encriptação simétrica (por exemplo, AES) e a encriptação assimétrica (por exemplo, RSA) para proteger a comunicação entre dois pontos finais.

Para melhor robustecer a sua resposta, forneça trechos de código (ou pseudo-código) para ambos os métodos de encriptação e explique as vantagens e desvantagens de cada abordagem no seu relatório.

4. Reflexão sobre a estratégia de segurança

Conclua o seu relatório com uma secção que discuta a estratégia global de segurança para a rede. Esta secção deve incluir um resumo das principais vulnerabilidades resolvidas, quaisquer preocupações de segurança remanescentes e recomendações para futuras melhorias de segurança.

O relatório a entregar deve apresentar a seguinte estrutura:

1. Introdução

Forneça uma breve descrição geral dos objetivos do trabalho e do âmbito da sua análise.

2. Análise da rede e das ameaças

Análise do diagrama de rede: Descreva a estrutura da rede, os principais componentes e as possíveis vulnerabilidades.

Identificação de ameaças: Listar as ameaças por categorias (confidencialidade, integridade, disponibilidade).

Diagrama de árvore de ataque: Representação visual de possíveis caminhos de ataque.

3. Proposta de controlo de segurança

Controlos propostos: Descrever cada controlo em pormenor, relacionando-o com as vulnerabilidades específicas abordadas.

Justificação: Explicar como cada controlo se alinha com os princípios de segurança e reduz riscos específicos.

4. Implementação da solução criptográfica

Encriptação simétrica: Fornecer o trecho de código (ou pseudo-código), uma explicação da implementação e as vantagens/desvantagens.

Encriptação assimétrica: Fornecer o trecho de código (ou pseudo-código), uma explicação da implementação e vantagens/desvantagens.

5. Conclusão e reflexão sobre a estratégia

Faça um resumo das medidas de segurança, discuta a sua eficácia e identifique eventuais limitações.

Reflita sobre a forma como a sua estratégia cumpre os requisitos de segurança e sugira melhorias.

6. Referências

Inclua todas as fontes utilizadas para a sua investigação, referências de código e quaisquer materiais académicos ou técnicos consultados. Indicar se recorreu a algum motor de IA.

Algumas notas finais: - Atenção à estrutura do documento e respetivo conteúdo; - Atenção ao nível do português utilizado; - Atenção às referências bibliográficas; - Atenção aos erros ortográficos; - Atenção à reutilização de código obtido diretamente na web (nota: eu também conheço essas fontes!); - Atenção às "reutilizações" de textos de livros, artigos, outros trabalhos ou ChatGPT. Plágios serão penalizados!

Recursos

Utilize os recursos à sua disposição, nomeadamente:

1. Fórum específico do eFolio A
2. Manual recomendado
3. Website do NIST (National Institute of Standards and Technology) Special Publications on Network Security and Cryptography.
4. Website do OWASP (Open Web Application Security Project) resources for understanding and addressing vulnerabilities.
5. Recursos sobre árvores de ataque:
    a. https://www.practical-devsecops.com/threat-modeling-using-attack-trees/
    b. https://www.mytechiebits.com/AttackTrees
    c. https://www.ncsc.gov.uk/collection/risk-management/using-attack-trees-to-understand-cyber-security-risk

6. Ainda sobre árvores de ataque: (complementar) Shostack A. (2014). Threat Modeling Designing for Security. Wiley. (pp. 87-100)

Critérios de avaliação e cotação

Na avaliação do trabalho serão tidos em consideração os seguintes critérios e cotações:

Critério	Descrição	Peso
Análise da rede e das ameaças	Exaustividade e exatidão das ameaças identificadas e da árvore de ataque.	20%
Proposta de controlo de segurança	Profundidade, relevância e justificação dos controlos de segurança propostos.	25%
Implementação da solução criptográfica	Exatidão e funcionalidade das soluções de encriptação, clareza do código e qualidade das explicações fornecidas.	25%
Reflexão sobre a estratégia	Resumo perspicaz da estratégia de segurança, incluindo limitações e melhorias futuras.	15%
Estrutura e Qualidade do relatório	Clareza, organização, gramática e respeito pela estrutura do relatório.	15%

Total: 4 pontos = 4 valores

Normas a respeitar

Deve redigir o seu relatório na Folha de Resolução disponibilizada na turma e preencher todos os dados do cabeçalho.

Todas as páginas do documento devem ser numeradas.

O seu relatório não deve ultrapassar 10 páginas A4 (excluindo a folha de rosto) redigidas em Arial, tamanho de letra 11. O espaçamento entre linhas deve corresponder a 1,5 linhas.

Nomeie o ficheiro com o seu número de estudante, seguido da identificação do E-fólio, segundo o exemplo apresentado: 000000efolioA.

Deve carregar os ficheiros para a plataforma no dispositivo E-fólio A até à data e hora limite de entrega. Evite a entrega próximo da hora limite para se precaver contra eventuais problemas. O ficheiro a enviar não deve exceder 8 MB.

Votos de bom trabalho!

Henrique S. Mamede