E-fólio A | Folha de resolução para E-fólio

UNIDADE CURRICULAR: Segurança em Redes e Computadores

CÓDIGO: 21181

DOCENTE: Henrique S. Mamede

A preencher pelo estudante

NOME: Luís Carlos Crispim Pereira

N.º DE ESTUDANTE: 2300163

CURSO: LEI – Licenciatura em Engenharia Informática

DATA DE ENTREGA: 16/11/25

TRABALHO / RESOLUÇÃO:

1. Introdução

Este e-fólio tem como objetivo analisar a segurança da infraestrutura de rede disponibilizada, identificando vulnerabilidades, avaliando possíveis vetores de ataque e propondo controlos que reduzam o risco para níveis aceitáveis. A abordagem segue princípios como privilégio mínimo, defesa em profundidade e gestão da superfície de ataque, garantindo uma visão estruturada das necessidades de proteção. O trabalho inclui também a demonstração de mecanismos de criptografia, com exemplos práticos de encriptação simétrica e assimétrica aplicáveis à proteção de dados. Por fim, a estratégia de segurança proposta é discutida à luz dos resultados obtidos.

2. Análise da rede e das ameaças

A infraestrutura apresentada segue uma arquitetura organizada por camadas, criada para controlar o tráfego desde a Internet até aos serviços internos. A ligação externa passa primeiro por um router, responsável pelo encaminhamento básico, e depois por uma firewall, que funciona como a primeira barreira contra acessos não autorizados. Após estes dispositivos, o tráfego é distribuído por um switch central, que liga os diferentes equipamentos e servidores da rede.

Na área mais exposta encontra-se uma DMZ (Demilitarized Zone), usada para isolar os serviços que precisam de estar acessíveis ao exterior. Este segmento aloja três servidores fundamentais da organização:

- Servidor de Base de Dados, que guarda a informação estruturada;
- Servidor Web/Aplicacional, que aloja serviços e páginas web;
- Servidor de Email, responsável pela comunicação eletrónica da organização.

A colocação destes serviços na DMZ impede que um eventual ataque externo tenha acesso direto à rede interna, reduzindo o risco de movimento lateral. O tráfego que circula entre estes componentes é ainda monitorizado por um IDS/IPS, que deteta e bloqueia atividades suspeitas.

O acesso dos utilizadores é feito através de duas redes distintas, ambas ligadas ao switch principal:

- LAN, constituída por equipamentos ligados por cabo, como computadores de secretária e impressoras;
- WLAN, que fornece acesso sem fios a dispositivos móveis através de um ponto de acesso.

A separação entre DMZ, LAN e WLAN permite aplicar políticas de segurança específicas a cada área e contribui para reduzir a superfície de ataque da rede.

Ameaças à Confidencialidade:

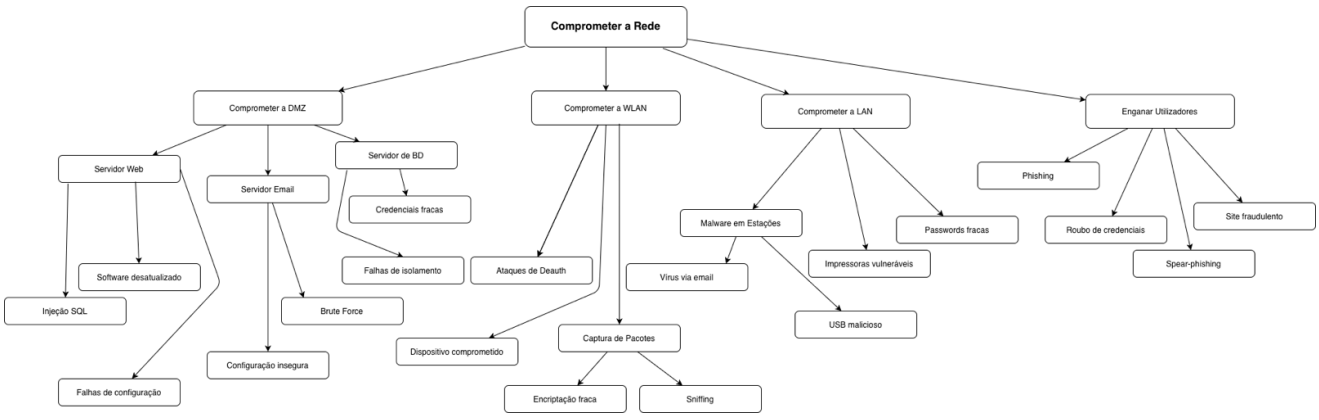
- Interceção de tráfego na WLAN devido a encriptação fraca ou palavras-passe previsíveis.
- Sniffing de comunicações entre utilizadores e servidores se não houver TLS.
- Acesso não autorizado a contas internas através de phishing ou reutilização de credenciais.
- Exposição de dados sensíveis na DMZ causada por má configuração de serviços públicos.
- Roubo de informação em dispositivos móveis não protegidos por bloqueio ou encriptação.

Ameaças à Integridade:

- Alteração de dados no servidor de Base de Dados por atacantes com credenciais obtidas indevidamente.
- Injeção de código ou comandos em aplicações Web vulneráveis na DMZ.
- Manipulação de ficheiros ou configurações na LAN por utilizadores com permissões excessivas.
- Modificação indevida de regras da firewall ou do IDS/IPS por falhas na proteção das contas administrativas.
- Propagação de malware que altera ficheiros ou parâmetros críticos do sistema.

Ameaças à Disponibilidade:

- Ataques DoS/DDoS dirigidos ao servidor Web, ao servidor de Email ou à firewall.
- Sobrecarga da ligação à Internet que impede o funcionamento normal dos serviços expostos.
- Interferência ou jamming na WLAN que interrompe o acesso sem fios.
- Falha no switch central que provoca interrupção total do acesso interno.
- Infeção por ransomware que bloqueia ficheiros essenciais e paralisa serviços dependentes.



3. Proposta de controlo de segurança

1. Ativar obrigatoriamente TLS/HTTPS em todas as comunicações entre utilizadores, servidores internos, servidor Web e servidor de Email. Incluir certificados válidos e renovação automática. Este controlo protege a Confidencialidade e a Integridade das comunicações, prevenindo ataques de sniffing, Man-in-the-Middle e captura de dados sensíveis na LAN e WLAN. Alinha-se com o princípio de Defesa em Profundidade, ao garantir que mesmo que a WLAN seja comprometida (ex.: encriptação fraca ou sniffing), os dados continuam protegidos.
2. Aplicar políticas de palavras-passe robustas, MFA (autenticação multifator) para contas administrativas e renovação periódica das credenciais. Implementar bloqueio após tentativas falhadas. Este controlo reduz drasticamente ataques de brute force, reutilização de credenciais, phishing e acessos não autorizados. Segue o princípio de Privilégio Mínimo, ao assegurar que só utilizadores legítimos acedem aos recursos e que o impacto de credenciais roubadas é limitado.
3. Criar regras claras de firewall para limitar o fluxo de tráfego entre a DMZ, a LAN e a WLAN. Restringir comunicações apenas ao estritamente necessário (por exemplo: DMZ → BD apenas na porta de base de dados). A segmentação impede movimento lateral depois de uma intrusão, reduzindo a superfície de ataque e protegendo os servidores críticos. Alinha-se com Defesa em Profundidade e Contenção de Danos, mitigando ataques como malware em estações, dispositivos comprometidos ou exploração de vulnerabilidades na DMZ.
4. Aplicar patches de segurança, remover serviços desnecessários, aplicar configurações seguras (hardening) e utilizar mecanismos de monitorização (IDS/IPS) com regras atualizadas. Este controlo mitiga vulnerabilidades como software desatualizado, falhas de configuração, injeção SQL, e ataques ao servidor Web e servidor de Email. Cumpre o princípio de Segurança por Configuração Adequada, garantindo que serviços expostos na DMZ apresentam a menor superfície de ataque possível.
5. Configurar a WLAN com WPA3 ou, no mínimo, WPA2 com password forte e rotação periódica. Ativar Client Isolation para impedir comunicação direta entre dispositivos. Monitorizar ataques de deauth. Mitiga riscos como encriptação fraca, sniffing, captura de pacotes e ataques de desautenticação. Alinha-se com Confidencialidade e Disponibilidade, assegurando que a rede sem fios não se torna porta de entrada para a LAN.
6. Instalar soluções EDR/antivírus em todos os equipamentos da LAN, bloquear dispositivos USB não autorizados, e filtrar anexos de email suspeitos. Reduz riscos de malware em estações, vírus via email, USB malicioso, e compromissos internos que conduzam a movimento lateral. Corresponde a Defesa em Profundidade, protegendo a LAN mesmo que um utilizador clique num link malicioso.
7. Promover formação periódica sobre phishing, engenharia social, passwords seguras e boas práticas de utilização de sistemas. Mitiga diretamente ameaças como phishing, spear-phishing, sites fraudulentos, roubo de credenciais. Reflete o princípio Human Firewall, reduzindo a principal superfície de ataque, os utilizadores.

4. Implementação da solução criptográfica

Encriptação simétrica

```
from cryptography.hazmat.primitives.ciphers.aead import AESGCM
import os

data = b"message to encrypt"
aad = b"authenticated but not encrypted data"
key = AESGCM.generate_key(bit_length=128)
aesgcm = AESGCM(key)
nonce = os.urandom(12)
ct = aesgcm.encrypt(nonce, data, aad)
pt = aesgcm.decrypt(nonce, ct, aad)

print("Ciphertext:", ct)
print("Decrypted:", pt)
```

A implementação utiliza o algoritmo AES no modo GCM, disponibilizado pela biblioteca oficial cryptography do Python, que é atualmente uma das soluções mais seguras e recomendadas para encriptação simétrica. O processo começa com a definição dos dados a proteger, representados em formato binário, e com a criação opcional de dados autenticados mas não cifrados (AAD), que permitem garantir a integridade de metadados associados à mensagem. De seguida é gerada automaticamente uma chave de 128 bits através da função AESGCM.generate_key(), garantindo que o segredo utilizado na encriptação possui a entropia necessária para resistir a ataques de força bruta.

Com a chave criada, é instanciado um objeto AESGCM, que será responsável pelas operações de encriptação e desencriptação. O algoritmo AES-GCM requer um nonce, um valor aleatório que não pode repetir-se para a mesma chave, sendo por isso gerado através de os.urandom(12), que fornece 96 bits de aleatoriedade, o tamanho recomendado pelo NIST. É este nonce que assegura que duas mensagens iguais nunca produzem o mesmo resultado cifrado, impedindo ataques baseados na repetição de padrões.

A encriptação é realizada com a função encrypt(nonce, data, aad), que devolve um único bloco que combina o texto cifrado e a authentication tag, responsável por garantir que a mensagem não foi alterada durante a transmissão. A desencriptação é feita com o método simétrico decrypt(), que recebe exatamente o mesmo nonce, a mesma chave e os mesmos dados AAD. Se qualquer elemento tiver sido modificado, a operação falha automaticamente e a biblioteca levanta uma exceção, o que impede a utilização de dados adulterados.

Esta abordagem oferece simultaneamente confidencialidade, integridade e autenticidade das mensagens, sem necessidade de mecanismos adicionais. O modo GCM é amplamente utilizado em protocolos modernos como TLS 1.3, sendo considerado seguro, eficiente e adequado para praticamente qualquer aplicação que exija proteção de dados sensíveis.

Vantagens da encriptação simétrica:

- É muito rápida e eficiente, permitindo cifrar grandes volumes de dados com baixa utilização de recursos.
- A implementação é simples, exigindo apenas uma chave secreta comum entre as partes.
- É considerada altamente segura quando utilizada com chaves fortes e nonces únicos.
- O modo GCM fornece encriptação e autenticação ao mesmo tempo, garantindo confidencialidade e integridade numa única operação.
- É amplamente suportada em protocolos modernos (TLS 1.3, IPsec, SSH).

Desvantagens da encriptação simétrica:

- Requer um método seguro de troca da chave secreta, o que pode ser difícil sem outro mecanismo (ex.: assimétrico).
- Se a chave for comprometida, o atacante consegue decifrar todas as mensagens, passadas e futuras.
- O uso incorreto do nonce (por exemplo, reutilização) compromete completamente a segurança.
- Não fornece autenticação das partes, apenas do conteúdo.
- Não permite que duas partes se comuniquem de forma segura sem terem previamente partilhado a chave.

Encriptação assimétrica:

```
from cryptography.hazmat.primitives.asymmetric import rsa, padding
from cryptography.hazmat.primitives import hashes

private_key = rsa.generate_private_key(
    public_exponent=65537,
    key_size=2048,
)
public_key = private_key.public_key()

message = b"encrypted data"
ciphertext = public_key.encrypt(
    message,
    padding.OAEP(
        mgf=padding.MGF1(algorithm=hashes.SHA256()),
        algorithm=hashes.SHA256(),
        label=None
    )
)

plaintext = private_key.decrypt(
    ciphertext,
    padding.OAEP(
        mgf=padding.MGF1(algorithm=hashes.SHA256()),
        algorithm=hashes.SHA256(),
        label=None
    )
)
```

A solução apresentada utiliza o algoritmo RSA tal como implementado pela biblioteca cryptography, seguindo exatamente as práticas recomendadas na documentação oficial. O processo começa pela geração de um par de chaves assimétricas, composto por uma chave privada e uma chave pública. A chave privada é criada com um tamanho de 2048 bits e um expoente público de 65537, que constitui o valor mais utilizado e considerado seguro pela comunidade criptográfica. A partir desta chave privada, é derivada automaticamente a correspondente chave pública, que será utilizada para a encriptação dos dados.

A encriptação é efetuada exclusivamente com a chave pública, garantindo que apenas o detentor da chave privada consegue recuperar a informação original. Para proteger o processo de encriptação contra ataques criptográficos modernos, é aplicado o mecanismo OAEP (Optimal Asymmetric Encryption Padding), que utiliza a função de hash SHA-256 tanto no preenchimento como no mask generation function (MGF1). Este esquema é considerado seguro e é o recomendado em praticamente todos os contextos de uso de RSA na atualidade, incluindo normas NIST e documentação académica.

O resultado da encriptação é um bloco de dados cifrados que pode ser transmitido ou armazenado de forma segura, uma vez que sem a chave privada não é possível obter o texto original. A desencriptação ocorre exclusivamente com a chave privada, que aplica o mesmo esquema OAEP para desfazer o processo e revelar o texto simples. Uma vez que a chave privada nunca deve ser partilhada, este mecanismo garante confidencialidade mesmo que os dados cifrados circulem por canais inseguros. Todo o procedimento segue o paradigma clássico da criptografia assimétrica: encriptação com a chave pública e desencriptação com a chave privada, assegurando isolamento, confidencialidade e controlo rigoroso sobre quem tem acesso aos dados originais.

Vantagens da encriptação assimétrica:

- Permite troca segura de chaves sem necessidade de contacto prévio, ao contrário da encriptação simétrica.
- Suporta assinaturas digitais, garantindo autenticidade e não-repúdio das mensagens.
- A chave pública pode ser distribuída livremente, facilitando a escala e gestão em sistemas grandes.
- Reduz o risco associado ao compromisso de uma chave, pois a chave privada nunca é partilhada.
- Adequada para estabelecer sessões seguras iniciais (ex.: TLS), antes de passar para encriptação simétrica mais rápida.

Desvantagens da encriptação assimétrica:

- É muito mais lenta do que a encriptação simétrica, tornando-a inadequada para grandes volumes de dados.
- Requer chaves maiores para atingir níveis de segurança equivalentes, aumentando a sobrecarga computacional.
- Depende de infraestruturas de confiança (como certificados e PKI) para garantir que as chaves públicas são legítimas.
- Implementações inseguras podem permitir ataques como man-in-the-middle se a chave pública não for validada.
- Um compromisso da chave privada compromete todo o sistema, sendo necessária gestão rigorosa e armazenamento seguro.

5. Conclusão e reflexão sobre a estratégia

Ao longo deste trabalho foi possível identificar várias fragilidades na infraestrutura analisada e propor controlos capazes de mitigar riscos associados à confidencialidade, integridade e disponibilidade dos sistemas. As medidas implementadas seguem princípios essenciais, como privilégio mínimo, defesa em profundidade e segmentação adequada da rede, permitindo reduzir a superfície de ataque e dificultar movimentos laterais.

Entre as medidas propostas destacam-se as melhorias na configuração da firewall e do IDS/IPS, a segmentação clara entre LAN, WLAN e DMZ, as políticas de gestão de credenciais mais rigorosas, a encriptação de comunicações, a atualização regular de sistemas, a proteção contra malware e formação dos utilizadores. Estas ações atuam sobre três dimensões fundamentais (técnica, física e humana) criando um conjunto equilibrado de mecanismos preventivos e reativos.

Apesar de a estratégia reforçar significativamente a postura de segurança da organização, é importante reconhecer que nenhum conjunto de medidas garante proteção total. A evolução constante das ameaças, aliada ao fator humano, exige revisões periódicas, monitorização contínua e atualizações regulares das políticas e tecnologias usadas. A realização de auditorias internas, análise de logs, testes de intrusão e verificações regulares da configuração da rede são passos que deverão complementar o plano proposto.

De forma geral, a solução apresentada cumpre os requisitos essenciais definidos para este trabalho e estabelece uma base sólida para a segurança da infraestrutura. Contudo, a resiliência a longo prazo depende da capacidade da organização de manter estes controlos atualizados, promover cultura de segurança entre os colaboradores e adaptar-se a novas ameaças de forma contínua.

6. Referências

Cisco Systems. (2023). Cisco Networking Essentials. Cisco Press.

NIST – National Institute of Standards and Technology. (2018). Guide to General Server Security (SP 800-123).

NIST – National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems (SP 800-53 Rev.5).

OWASP Foundation. (2024). OWASP Top 10 – Web Application Security Risks.

Shostack, A. (2014). Threat Modeling: Designing for Security. Wiley.

NCSC – National Cyber Security Centre. (2023). Using Attack Trees to Understand Cyber Security Risk. Disponível em: https://www.ncsc.gov.uk/collection/risk-management/using-attack-trees-to-understand-cyber-security-risk

Practical DevSecOps. (2022). Threat Modeling Using Attack Trees. Disponível em: https://www.practical-devsecops.com/threat-modeling-using-attack-trees/

MyTechieBits. (2023). Attack Trees Explained. Disponível em: https://www.mytechiebits.com/AttackTrees

Python Cryptography Library – Documentation. (2024). AESGCM. Disponível em: https://cryptography.io/en/latest/hazmat/primitives/aead/#aesgcm

Python Cryptography Library – Documentation. (2024). RSA – Asymmetric Encryption. Disponível em: https://cryptography.io/en/latest/hazmat/primitives/asymmetric/rsa/

Houve utilização pontual de ferramentas de IA generativa para apoio à redação. A análise técnica, os conteúdos de segurança e o código foram totalmente elaborados e validados pelo autor.