Threat Modeling and security assessment of a NAS storage system in a small office network

Messaoudi Leila

ULB UNIVERSITÉ LIBRE DE BRUXELLES

Professor : Mühlberg Jan Tobias

ELEC-H550 Embedded System Security

16 December 2025

Summary

- Scope and methodology
- DFD
- STRIDE
- Nmap and Nessus
- Matrice of impact
- Mitigations

Messaoudi Leila

Scope and Methodology

3-Phase Hybrid Approach

Reconnaissance
Black Box

Nmap

Attack surface mapping

Validation
Grey Box

Nessus

Vulnerability qualification

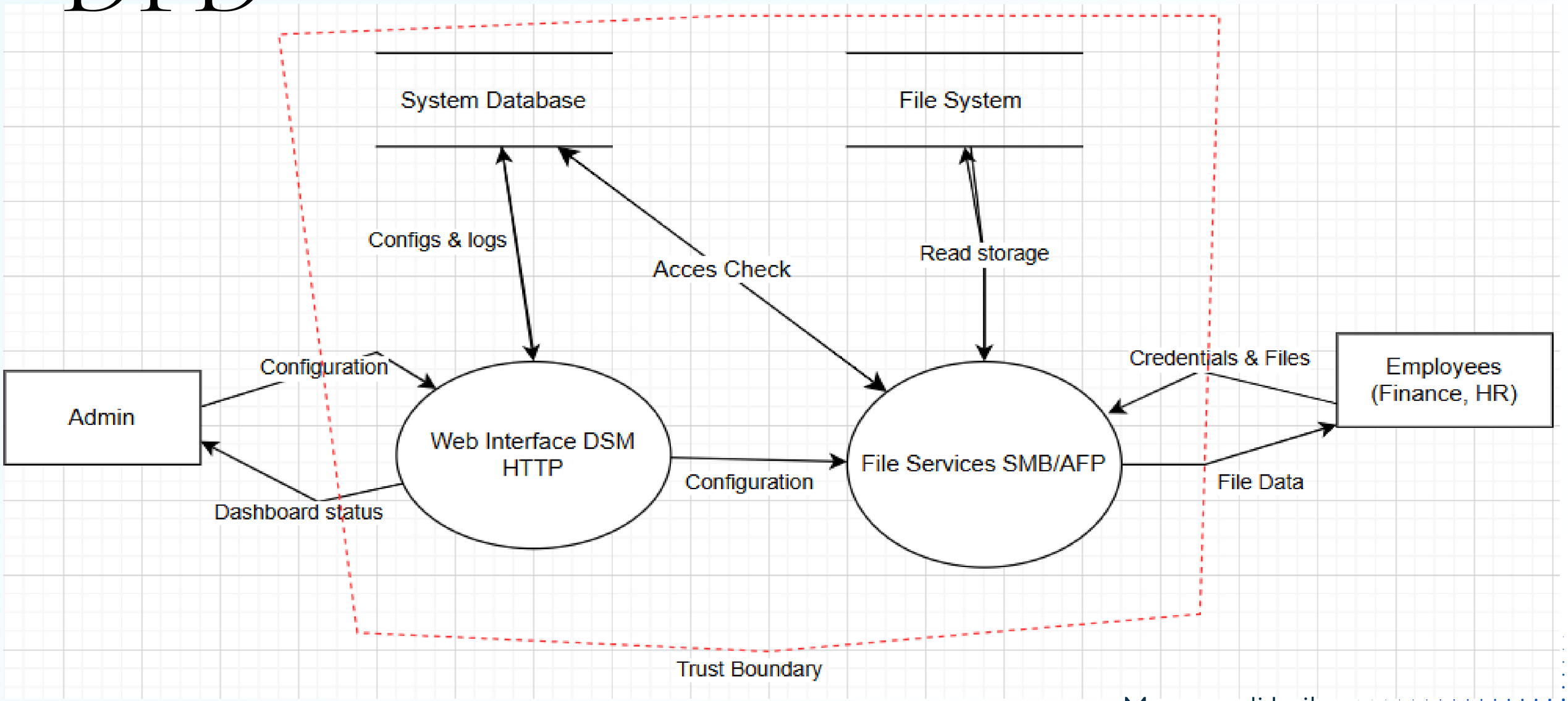
Modeling
White Box

STRIDE

Technical and organizational threat analysis

Messaoudi Leila

DFD



Messaoudi Leila

STRIDE Threat Model – Part 1

Focus: Identity & Integrity Risks

Spoofing

The Flaw:
Generic shared account "Compta" used by everyone.

Concrete Example:

"Audit logs show 'User Compta' logged in at 9:00 AM. It is impossible to know if it was Alice, Bob, or an attacker."

Tampering

The Flaw:
SMB Signing disabled (Nmap confirmed).

Concrete Example:

"A Ransomware infects one PC. Because write permissions are too broad, it encrypts the entire shared 'Finance' folder via the network."

Repudiation

The Flaw:
No audit logs enabled for file operations.

Concrete Example:

"An important Excel invoice is deleted. Management asks 'Who did this?'. The system cannot answer. There is no proof, so no accountability."

Messaoudi Leila

STRIDE Threat Model – Part 2

Focus: Confidentiality & Authorization Risks

Info. Disclosure

The Flaw:
AFP protocol sends passwords in Cleartext.

Concrete Example:

"Nmap output showed 'UAM: Cleartxt'. An attacker using Wireshark on the office Wi-Fi could read the admin password instantly."

Denial of Service

The Flaw:
Unnecessary services exposed (UPnP, AFP).

Concrete Example:

"Nmap flagged the 'Apache Killer' script. Even if patched, exposing the web interface internally increases the risk of the server crashing under load."

Elevation of Priv.

The Flaw:
Trust based on location, not identity.

Concrete Example:

"An intern left alone in the HR office can access sensitive payroll files because the PC is already authenticated to the NAS."

Messaoudi Leila

Scan Nmap

Attack Surface – Nmap Results

Nmap Scan Findings

AFP (TCP 548) — CRITICAL

⚠ Cleartext Authentication

Result: 'Cleartxt Passwrd' detected

HTTP Script Alert (NSE) — CRITICAL

Apache Killer (CVE-2011-3192)

Result: Nmap flagged potential DoS vulnerability

SMB (TCP 445) — HIGH

Message signing disabled

HTTP (TCP 5000) — HIGH

Unencrypted Admin Interface

Analysis & Context

Scanning revealed an unnecessarily large attack surface for an internal file server.

- **Legacy Protocols:** AFP is active despite being obsolete.
- **Script Alert:** NSE scripts flagged a critical DoS flaw (Apache Killer) requiring immediate verification.
- **Weak Config:** No SMB signing & HTTP management.

Next Step: Verification

Nmap indicates potential critical flaws. We must now run Nessus to confirm if the DoS risk is real or a false positive.

Messaoudi Leila

Scan Nessus

Nessus Analysis – Validation & False Positives

False Positive Dismissed

CVE-2011-3192 "Apache Killer" — Dismissed

Nmap Alert: Critical DoS Vulnerability

Explanation: Security backporting applied by Synology

Apache version patched, banner not updated

Conclusion: Low software DoS risk

Configuration Validations

SMB Signing — Medium Severity

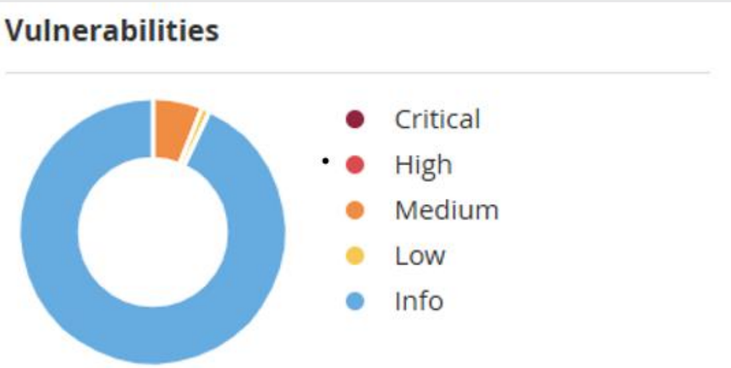
Signing disabled → MITM Risk

SSL Certificates — Medium Severity

Self-signed certificates → Spoofing risk

Results Summary

0 confirmed critical software vulnerabilities. Main risks: Secure configuration review required.



Messaoudi Leila

Risk Assessment – Prioritization

Priority	Threat	Likelihood	Impact	Rationale
CRITICAL	AFP Cleartext Auth	Very High	Critical	Credentials circulating in cleartext. Immediate compromise possible.
HIGH	Repudiation (No Logs)	High	High	No audit trail available for internal incidents. Legal risk.
HIGH	SMB Signing Disabled	Medium	High	Risk of silent data tampering (financial records).
MEDIUM	Spoofing (Accounts)	High	Medium	Poor cyber hygiene (shared accounts), complicates investigations.
LOW	Software DoS	Very Low	High	Risk ruled out by Nessus validation (System patched).

Risk-based Prioritization

The matrix guides the action plan towards the most probable and impactful threats.

Messaoudi Leila

Mitigations

Immediate Actions – Technical Hardening

Disable AFP (TCP 548)

Migration to SMBv3

Complete deactivation of the obsolete AFP service

Migrate all client workstations (Mac) to secure SMBv3

Priority: Critical

Enable SMB Signing

Server Configuration

Enforce packet signing on both client and server sides

Prevention of Man-in-the-Middle attacks

Priority: High

Enforce HTTPS

Forced Redirection

Redirect port 5000 (HTTP) to 5001 (HTTPS)

Install a valid certificate (Let's Encrypt)

Priority: High

Deploy a Valid Certificate

Let's Encrypt

Deployment of free public certificate

Enable HSTS to enforce encryption

Priority: Medium

Mitigations

Organizational Measures – Medium Term

Identity Management (IAM)

Remove Generic Accounts

Create unique named accounts for every employee

Ensures individual accountability for actions

Governance: IT + HR

Audit & Logging

Enable SMB Logging

Full logging of file transfer activities

Export to remote Syslog server for log integrity

Governance: IT

Principle of Least Privilege

Permission Review

Restrict write access to necessary users only

Protection against ransomware and accidental deletion

Governance: IT + Management

Ransomware Protection

Versioned Backups

3-2-1 Backup Strategy with restoration tests

Isolation of backups from the main network

Governance: IT + Management

Thank You!

Messaoudi Leila

Questions ?

Messaoudi Leila