

1.Introduction & Methodology

The modern era threat landscape is rapidly evolving. Corporate networks are prime targets for attackers. Proactive vulnerability management allows for optimized risk reduction improved security posture

Project Aim:
Explores the implementation of Nessus in real-world environment and evaluates its impact to target posture

Key Objectives:

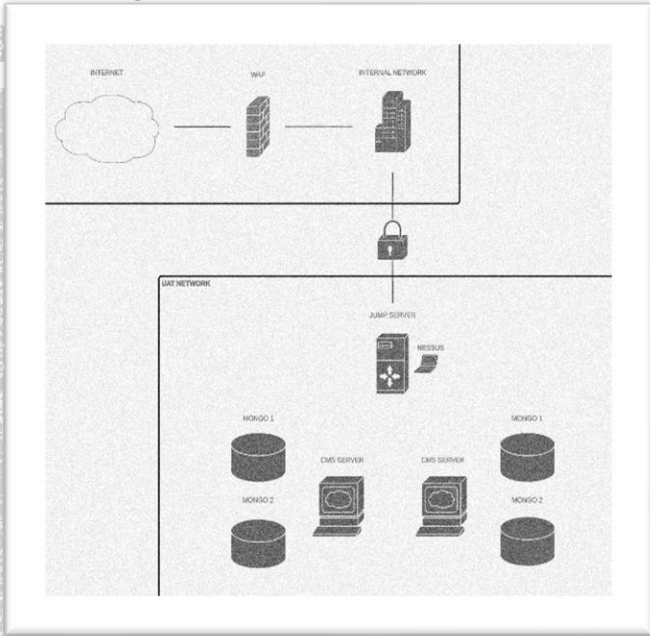
- ❑Research Nessus & best practice
- ❑Implement Nessus in real world network
- ❑Evaluate effect on target posture

Approach:

- Pragmatic
- Mixed Methods
- Experimental
- Cross sectional

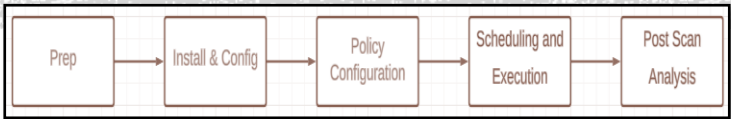
2.Design & Implementation

Target Network:



Host	Summary
Jump Server	Windows 2019 Server providing gateway to air-gapped network.
CMS	Windows 2019 servers running IIS
Database	Linux servers running MongoDB in replication

Implementation Strategy:



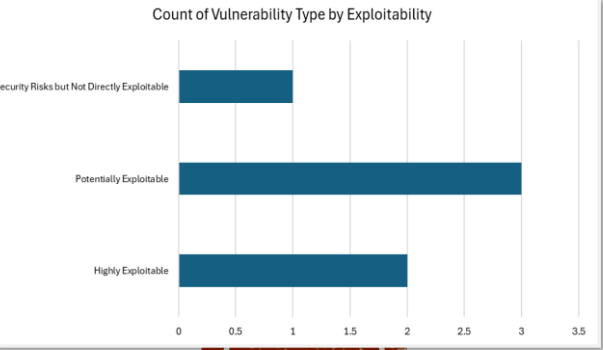
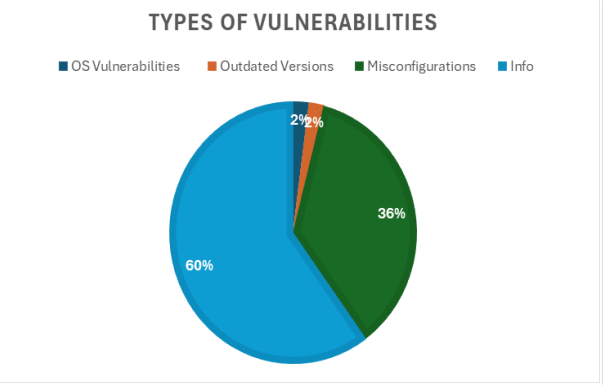
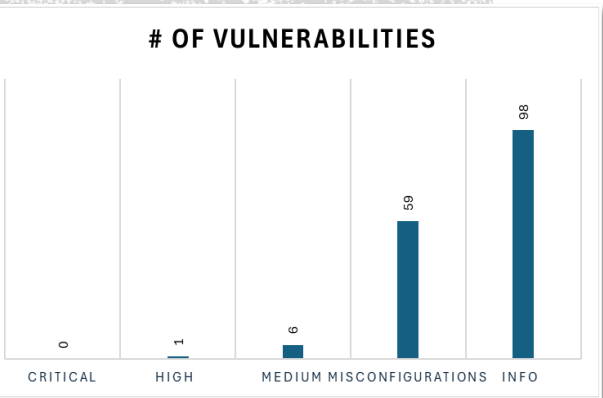
Implementation Challenges:

- Manual licensing
- Manual Plugin installation
- Host configuration

3.Testing & Evaluation

Key Evaluation Criteria:

- Coverage
- Severity & Type
- Remediation Success
- False Positives



Highlights

- Robust Detection
- Risk Prioritization
- Enhanced Awareness

Challenges:

- Scan Results
- Deployment conditions
- Scalability

4. Conclusion

- ✅ Implementation successfully identified and helped mitigate vulnerabilities
- ✅ Proved effective in positively impacting target networks security posture
- ✅ Demonstrated value added in pro-active assessments

Info

- David Cornelius
- Applied Cybersecurity and Networking
- University of Wales Trinity Saint David
- January 2025