

1. Introduction

Gold Builds serve as secure, standardised templates for deploying Windows Server systems, particularly in environments like the NHS that require consistency, security, and compliance. This project evaluates the design, implementation, and security posture of a Windows Server 2022 Gold Build.

2. Aims & Objectives

Aim: Develop a Windows Server 2022 Gold Image and evaluate through vulnerability assessments and penetration testing and applying remediations.

Objectives

1. Review best practices, standards, and frameworks for Windows Server hardening.
2. Implement and configure a Windows Server 2022 Gold Image, conducting security testing to evaluate whether it meets a gold standard.
3. Evaluate the effectiveness of the implemented security measures and provide recommendations for secure, standardised Gold Build deployment.

3. Literature Review

Legacy protocols (SMBv1 and TLS1.0/1.1) continue to pose a serious risk, along with misconfigurations in Firewalls, access controls, RDP setup, and authentication.

Upgrading from legacy encryption and implementing RBAC for permission management improves security. Compliance with frameworks and standards such as NIST SP 800-123, NCSC guidance, and ISO/IEC 27001 can also improve security.

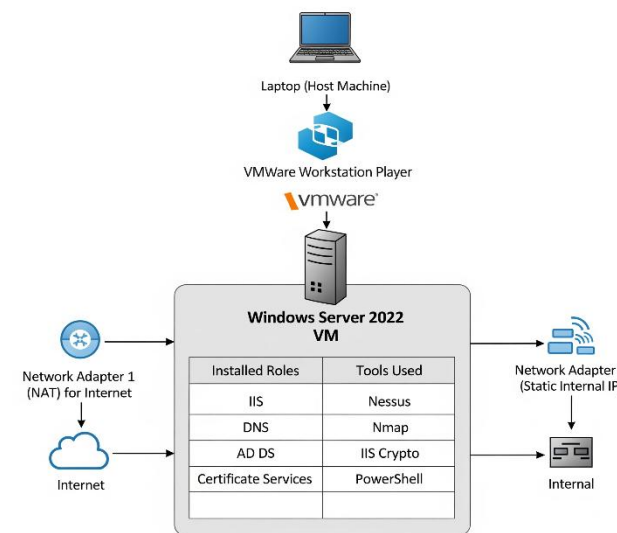
Regular vulnerability assessments using tools such as Nessus and Nmap, plus Penetration Testing.

Migration includes fees and compatibility checks but can greatly improve default security controls.

4. Design

Server Version: Windows Server 2022 (most common NHS rollout version).

Roles Installed: IIS Web Server, DNS, Active Directory (simulates realistic NHS environments).



5. Implementation

Windows 2022 server hosted on VMware Workstation (Isolated Environment).

PowerShell scripts and manual configuration for initial server build.

Common misconfigurations introduced unintentionally when implementing features, roles, and services.

Installed and utilised security tools: Nessus Essentials, Nmap, IIS Crypto, and PowerShell.

Remediated vulnerabilities discovered through scripts, policies, and tools.

Acknowledgements

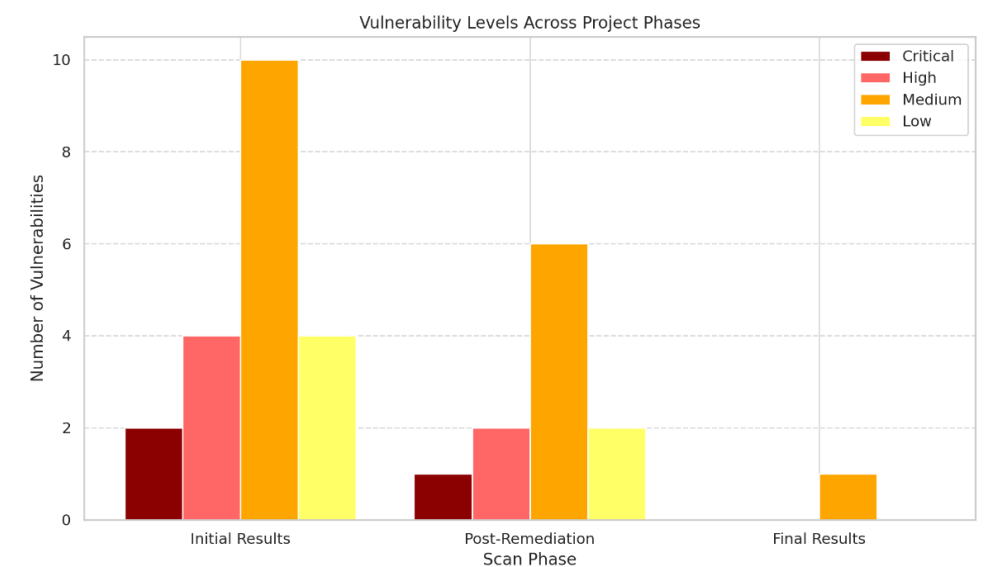
https://www.cisecurity.org/benchmark/microsoft_windows_server

<https://pages.nist.gov/800-63-3/sp800-63b.html>

<https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en>

6. Results

Security testing was conducted across three stages: initial setup, post-remediation, and final validation. The initial scan identified multiple critical, high, medium, and low vulnerabilities. After remediation and configuration changes, new issues were introduced, but the original issues were resolved. Final testing showed just one medium-severity issue remaining.



7. Conclusion

The project successfully implemented and evaluated a secure Gold Build aligned with best practices and NHS requirements. Security was improved significantly through staged testing and remediation. Literature insights were validated in practice — especially around common misconfigurations. Project objectives were met, but further work should explore 2025 builds, full CIS benchmark alignment, and real NHS infrastructure deployment.

8. Recommendations

- Develop a Windows Server 2025 Gold Build.
- Explore CIS benchmark integration.
- Test in a real-world NHS environment with enterprise tools.
- Automate AD cleanup scripts for security group management.