Design World Security Hardening Project Report

A Comprehensive Analysis of Vulnerability Assessment, Risk-Based Remediation, and Security Control Validation

Prepared for: Design World (DW)

Prepared by: Kayvon Karimi - CyberRealm Sentinels

Date: November 24, 2025

Project Duration: CYBR 514-516 Capstone Sequence

Table of Contents

Executive Summary

This comprehensive project report documents the complete lifecycle of Design World's cybersecurity hardening program, from initial vulnerability assessment through implementation and validation of security controls. Following completion of infrastructure penetration testing and vulnerability assessment, Design World engaged CyberRealm Sentinels to conduct comprehensive security hardening of their private enterprise cloud infrastructure.

Design World, a multinational engineering firm with 100 employees across San Diego, Hong Kong, and Brussels, operates a private enterprise cloud environment supporting design and engineering operations. The firm serves both commercial clients and US government customers, requiring NIST SP 800-53 compliance for continued contract eligibility. Vulnerability assessment and penetration testing revealed critical security exposures requiring immediate remediation to protect intellectual property and maintain regulatory compliance.

Key outcomes achieved include complete vulnerability remediation (35 vulnerabilities across all severity levels reduced to zero), full compliance achievement with NIST SP 800-53 and CIS Benchmarks, zero exploitable attack vectors remaining post-hardening as confirmed through penetration testing, established multi-layered defenses protecting design data and infrastructure, and demonstrated regulatory compliance meeting US government customer requirements.

This report provides detailed documentation of how security requirements were chosen through risk-based selection and framework alignment, implemented through structured technical execution and change management processes, and tested through multi-layer validation including vulnerability scanning, penetration testing, and compliance assessment. The analysis demonstrates complete traceability from vulnerability discovery through remediation validation, establishing a secure and compliant operational baseline.

1. Introduction and Business Context

1.1 Organization Overview:

Design World represents the merger of three independent engineering firms specializing in artistic structural support systems design. The organization operates with the following characteristics:

Geographic Distribution: Offices located in San Diego (United States), Hong Kong, and Brussels (Belgium), supporting a globally distributed workforce.

Workforce: 100 employees working across three continents, requiring secure remote collaboration capabilities.

Business Model: High-value intellectual property development in structural engineering, with design data representing core business assets.

Client Base: Mixed customer portfolio including commercial clients and US government customers. Government contracts mandate NIST SP 800-53 compliance as a contractual requirement.

Technical Infrastructure: Private enterprise cloud with VPN access via three regional cloud installations.

1.2 Infrastructure Vulnerability Assessment:

Design World completed infrastructure vulnerability assessment and penetration testing from September-October 2025. The assessment scope included all systems within the private enterprise cloud environment.

Assessment Methodology:

- Vulnerability scanning using Tenable Nessus Professional
- Authenticated credentialed scans with administrative access
- Comprehensive coverage of all in-scope systems (8 hosts)

- Full CVE database correlation for vulnerability identification

Initial Vulnerability Baseline:

The vulnerability assessment identified 35 total vulnerabilities distributed across severity levels:

Figure 1 - Initial Vulnerability Baseline

Critical	1 vulnerability
High	5 vulnerabilities
Medium	24 vulnerabilities
Low	5 vulnerabilities

The assessment revealed critical security exposures posing significant risk to intellectual property, operations, and client trust. The most urgent findings identified were:

- **Domain Controller Exposure** (172.16.1.205): Active Directory services including LDAP, Kerberos, SMB, and RDP accessible from untrusted networks, combined with exploitable SMBv1 vulnerabilities (MS17-010 / EternalBlue family). This exposure represented the highest risk with potential for full domain compromise.
- **Remote Desktop Protocol Risks**: Multiple Windows hosts exposing RDP (TCP/3389) without enforced Multi-Factor Authentication or Network Level Authentication, increasing likelihood of brute force attacks and lateral movement.
- **Weak Cryptographic Configurations**: Several systems supporting deprecated cipher suites (RC4, 3DES/SWEET32), exposing sensitive communications to interception and decryption.
- **Configuration and Patch Gaps**: Outdated system builds and inconsistent patching practices increasing susceptibility to widely known exploits.

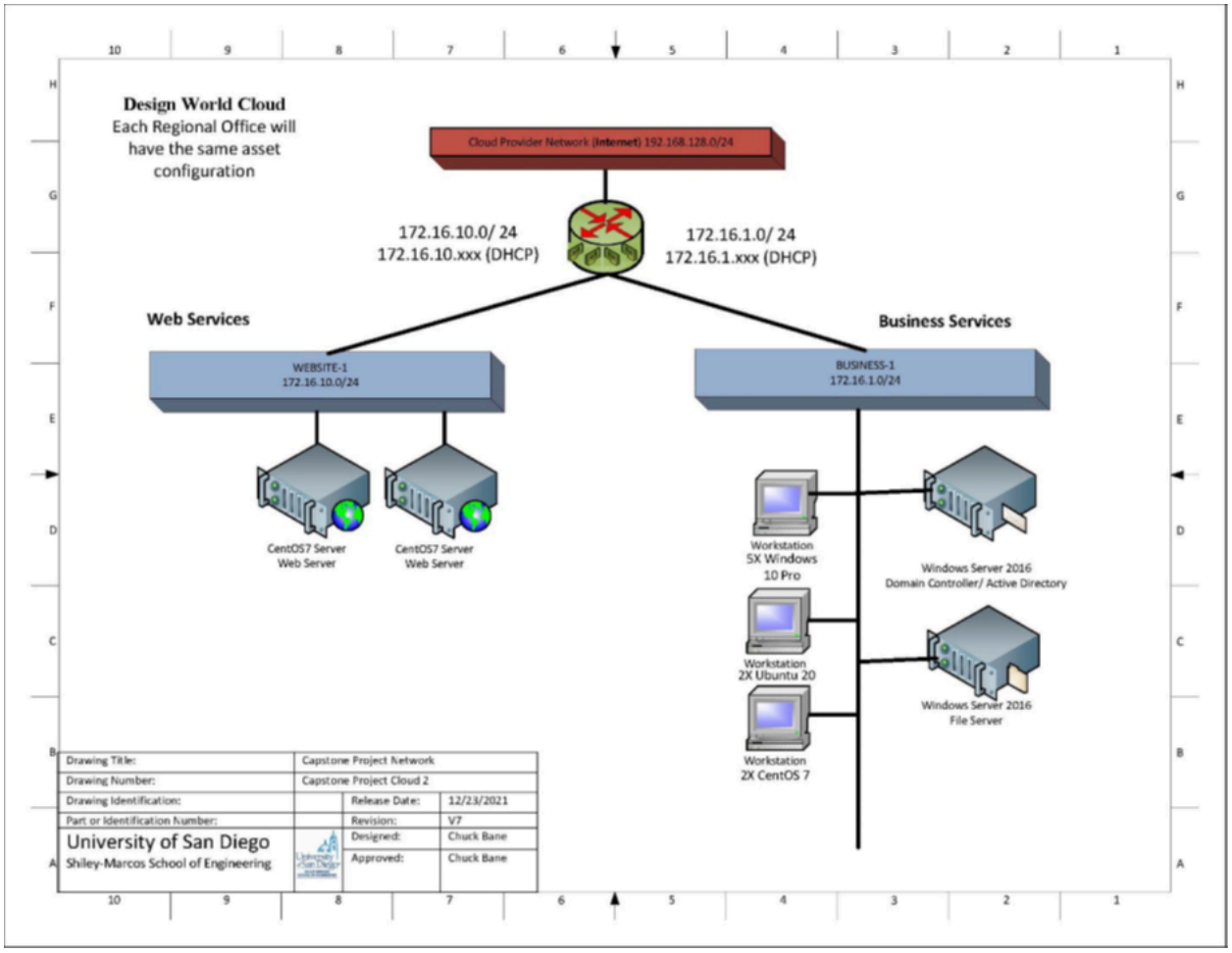
Technical Environment Pre-Hardening:

Design World's infrastructure consisted of eight virtualized systems operating on a private enterprise cloud with VPN-based remote access. The technical environment prior to hardening included the following components:

Figure 2 - System Architecture

Network Addressing	172.16.1.0/24 production network with 172.16.10.0/24 DHCP segment
Domain Infrastructure:	Windows Server 2016 Active Directory domain (DW-DC-OL1 at 172.16.1.205)
File Services:	Windows Server 2016 File Server (DW-FS-OL1 at 172.16.1.138)
User Workstations:	Windows 10 Pro systems (172.16.1.41, 172.16.1.93)
Linux Infrastructure:	Four Ubuntu 20.04 LTS servers providing general-purpose services (172.16.1.62, 172.16.1.94, 172.16.1.183, 172.16.1.202)
Access Control:	VPN-based remote access through cloud provider gateway
Authentication:	Active Directory with centralized credential management
Critical Gap:	The private enterprise cloud environment had not been comprehensively evaluated or documented according to enterprise security standards prior to the vulnerability assessment.

Figure 3 - Design World Private Cloud Network Topology



Note: Original cloud architecture provided by USD Cyber Cloud. During the CYBR-514/516 project sequence, Linux infrastructure was migrated from CentOS to Ubuntu 20.04 LTS as detailed in Figure 2.

1.3 Regulatory and Compliance Drivers:

The selection and implementation of security requirements was fundamentally driven by mandatory compliance obligations and business imperatives.

Primary Driver - US Government Customer Requirements:

- Design World provides services to US government clients

- Government contracts require NIST SP 800-53 compliance
- Failure to meet compliance standards would result in contract loss
- Regulatory penalties apply for non-compliance with federal security requirements

Secondary Drivers:

- Intellectual Property Protection: Design data represents core business assets requiring maximum security
- International Operations: Multi-jurisdictional regulatory considerations for global operations
- Industry Standards: Engineering sector best practices and professional liability requirements
- Insurance Requirements: Cyber insurance policy mandates for adequate security control implementation

Business Impact of Unmitigated Vulnerabilities:

If left unaddressed, the identified vulnerabilities could enable attackers to:

- Gain domain-wide control through Domain Controller compromise
- Exfiltrate sensitive design assets and intellectual property
- Deploy ransomware affecting business operations
- Disrupt operations across all geographic locations

The reputational and regulatory consequences of exploitation would pose severe business risk including loss of government contracts, regulatory penalties, and damage to client trust.

---

2. Security Requirements: Selection and Justification (CHOSEN)

This section documents the methodology for security requirement selection, the risk-based decision process, and the compliance frameworks that guided requirement prioritization.

2.1 Requirements Discovery and Vulnerability Assessment:

The security requirements process began with comprehensive vulnerability discovery using industry-standard tools and methodologies.

Discovery Methodology:

1. **Tool**: Tenable Nessus Professional vulnerability scanner
2. **Scan** Type: Authenticated credentialed scans with administrative access
3. **Coverage**: All eight in-scope systems across Windows and Linux platforms
4. **Plugin Set**: Full vulnerability detection with CVE database correlation
5. **Timeframe**: Initial baseline scans conducted September-October 2025

Initial Vulnerability Distribution by Host:

The vulnerability assessment revealed that risk was concentrated on the Domain Controller, with additional exposures distributed across file servers, workstations, and Linux systems.

Figure 4 - Initial Vulnerability Distribution by Host

Host	Critical	High	Medium	Low
172.16.1.205 (Domain Controller)	1	5	6	0
172.16.1.138 (File Server)	0	1	4	1
172.16.1.41 (Workstation)	0	0	2	1
172.16.1.93	0	0	2	1

(Workstation)				
172.16.1.62 (Linux Server)	0	0	3	1
172.16.1.94 (Linux Server)	0	0	3	1
172.16.1.183 (Linux Server)	0	0	3	1
172.16.1.202 (Linux Server)	0	0	3	1
TOTAL	**1**	**5**	**24**	**5**

Aggregate Risk Assessment:

- Total Vulnerabilities: 35
- Overall Risk Level: Critical (driven by Domain Controller exposure)
- Business Impact: Unacceptable risk to intellectual property and operations

2.2 Critical Risk Analysis and Crown Jewel Assessment:

The security engineering team conducted crown jewel analysis to prioritize requirements based on potential impact to Design World's core business assets.

Crown Jewel Asset Identification:

1. Design Intellectual Property - Stored on file servers and user workstations
2. Active Directory Domain - Controls authentication to all resources
3. Design Application Access - CAD and structural design tools
4. Client Communication Channels - Secure collaboration capabilities

Critical Vulnerability Analysis - Domain Controller Exposure (172.16.1.205)

This single vulnerability represented the highest risk to the entire environment.

Vulnerability Details:

- Asset: DW-DC-OL1 (Domain Controller)
- CVE References: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145 (MS17-010)
- Exploit Family: EternalBlue, EternalChampion, EternalRomance, EternalSynergy
- CVSS Score: 9.8 (Critical severity)
- Known Exploits: WannaCry, Petya, EternalRocks ransomware

Risk and Impact Analysis:

If exploited, the SMBv1 vulnerability would enable remote code execution on the Domain Controller, leading to full domain compromise with access to all systems, data, and credentials. Complete intellectual property exfiltration and ransomware deployment across the entire environment would be possible.

Business consequences would be severe: immediate total domain compromise giving attackers access to all systems, short-term exfiltration of all design intellectual property, and long-term loss of government contracts, reputation damage, and potential business failure.

Requirement Decisions Based on Critical Risk:

This single critical exposure mandated immediate selection of the following requirements:

- SMBv1 protocol disablement
- Microsoft MS17-010 security patching
- Network segmentation and firewall controls for Active Directory ports
- Active Directory hardening procedures

High-Risk Exposures: RDP and Cryptographic Weaknesses

Remote Desktop Protocol Exposure Analysis:

Figure 5 - Host identification with RDP security deficiences.

Host	**Exposure**
172.16.1.205 (Domain Controller)	RDP exposed without MFA or NLA, accessible from VPN subnet
172.16.1.138 (File Server)	RDP exposed without MFA or NLA, hosts sensitive IP
172.16.1.41 (User Workstation)	Direct RDP exposure, design applications present
172.16.1.93 (User Workstation)	Direct RDP exposure, design applications present

Attack Scenario:

Attacker on VPN conducts RDP brute force attack, compromises workstation, performs lateral movement to Domain Controller, achieves full network access.

Requirements Selected for RDP Hardening:

- Implement Network Level Authentication (NLA) - NIST IA-2
- Deploy Multi-Factor Authentication (MFA) for all RDP access - NIST IA-2(1)
- Restrict RDP to VPN/Jump Host subnets only - NIST AC-4
- Implement account lockout policies (5 failed attempts) - NIST AC-7

Weak Cryptographic Configuration Analysis:

Multiple systems identified supporting deprecated SSL/TLS protocols and cipher suites:

Identified Weaknesses:

- CVE-2016-2183 (SWEET32): 3DES cipher suite weakness, CVSS 7.5
- CVE-2013-2566, CVE-2015-2808 (Bar Mitzvah): RC4 cipher vulnerabilities, CVSS 5.9
- TLS 1.0/1.1: Deprecated protocols with known security weaknesses
- Self-Signed Certificates: No certificate authority validation chain

Affected Systems:

- Domain Controller (172.16.1.205): LDAP, Kerberos, RDP services
- File Server (172.16.1.138): SMB file shares, RDP access
- User Workstations: RDP and web services

Attack Impact Assessment:

- Man-in-the-middle (MITM) attacks on encrypted sessions
- Decryption of sensitive design file transfers
- Credential interception during authentication
- Government client communication compromise

Requirements Selected for Cryptographic Protection:

- Disable TLS 1.0 and TLS 1.1 protocols - NIST SC-13
- Remove RC4 and 3DES cipher suites - NIST SC-13
- Enforce TLS 1.2 minimum, TLS 1.3 preferred - NIST SC-13
- Deploy CA-issued certificates with SHA-256 signatures - NIST SC-12
- Implement AES-GCM cipher suites with forward secrecy - NIST SC-13

Configuration and Patch Management Gap Analysis:

The assessment identified significant gaps in patch management practices and system configurations requiring remediation.

Identified Deficiencies:

- Windows Systems: Inconsistent patch levels, missing critical security updates
- Linux Systems: Outdated package versions, kernel vulnerabilities present
- Configuration Drift: No centralized configuration management implemented
- Baseline Absence: No documented secure configuration standards

Requirements Selected for Patch Management:

- Establish 30-day SLA for critical patch deployment - NIST SI-2
- Implement Windows Server Update Services (WSUS) - NIST SI-2(2)
- Configure automated Ubuntu package updates - NIST SI-2
- Deploy CIS Benchmarks as configuration baseline - NIST CM-2
- Implement configuration drift monitoring - NIST CM-3

2.3 Framework-Driven Requirement Selection:

All security requirements were mapped to established security frameworks to ensure compliance with regulatory mandates and industry best practices.

NIST SP 800-53 Control Mapping:

All requirements mapped to NIST SP 800-53 Rev. 5 controls to ensure compliance with US government customer mandates.

Access Control Family (AC):

- AC-3 (Access Enforcement): Protect design IP through strict access controls
- AC-4 (Information Flow Enforcement): Network segmentation and firewall policies

- AC-7 (Unsuccessful Logon Attempts): Account lockout to prevent brute force

Identification and Authentication Family (IA):

- IA-2 (Identification and Authentication): Unique user accounts and strong authentication
- IA-2(1) (MFA for Privileged Accounts): Multi-factor authentication for administrators
- IA-2(2) (MFA for Network Access): Multi-factor authentication for VPN access
- IA-5 (Authenticator Management): Password complexity and key management

System and Communications Protection Family (SC):

- SC-7 (Boundary Protection): Firewalls and network segmentation
- SC-8 (Transmission Confidentiality): Encryption for data in transit
- SC-12 (Cryptographic Key Management): Certificate authority and key lifecycle
- SC-13 (Cryptographic Protection): Strong encryption algorithms only

System and Information Integrity Family (SI):

- SI-2 (Flaw Remediation): Timely patching of security vulnerabilities
- SI-3 (Malicious Code Protection): Antivirus and endpoint protection
- SI-4 (Information System Monitoring): SIEM and security event logging

Audit and Accountability Family (AU):

- AU-2 (Audit Events): Comprehensive security event logging
- AU-6 (Audit Review and Analysis): SIEM analysis and alerting
- AU-12 (Audit Generation): Automated log collection and forwarding

CIS Benchmarks Selection:

The team selected specific CIS Benchmarks as technical implementation guides:

- CIS Microsoft Windows Server 2016 Benchmark (Level 1): Domain Controller and File Server hardening
- CIS Microsoft Windows 10 Enterprise Benchmark (Level 1): Workstation security baseline
- CIS Ubuntu Linux 20.04 LTS Benchmark (Level 1): Server hardening procedures

Rationale:

CIS Benchmarks provide prescriptive, actionable technical controls that align with NIST requirements while offering clear step-by-step implementation guidance suitable for technical teams.

ISO/IEC 27001 Alignment:

Requirements cross-referenced with ISO/IEC 27001:2013 controls for international compliance alignment:

- A.9 (Access Control): Physical and logical access control mechanisms
- A.10 (Cryptography): Encryption and key management procedures
- A.12 (Operations Security): Vulnerability management and malware protection
- A.13 (Communications Security): Network security and information transfer controls
- A.14 (System Acquisition and Development): Security in development lifecycle

2.4 Requirements Prioritization Matrix:

The security engineering team developed risk-based prioritization framework for phased implementation:

Priority 1 - Critical (0-72 hours implementation):

- Domain Controller SMBv1 disablement and MS17-010 patching
- Active Directory port restrictions via firewall rules

- RDP access restriction to VPN/jump host subnets only
- Emergency vulnerability rescan for validation

Priority 2 - High (1-2 weeks implementation):

- Network Level Authentication (NLA) enforcement on all RDP services
- Multi-Factor Authentication (MFA) deployment for privileged accounts
- TLS 1.2/1.3 enforcement with weak cipher removal
- Certificate replacement with CA-issued certificates
- Windows security patch baseline establishment

Priority 3 - Medium (2-8 weeks implementation):

- Host-based firewall deployment (Windows Firewall, UFW)
- SIEM integration and security log forwarding
- Configuration management tool deployment
- Security monitoring procedures establishment
- Endpoint Detection and Response (EDR) evaluation

Priority 4 - Long-term (2-6 months):

- Zero Trust architecture expansion
- Network micro-segmentation implementation
- Data Loss Prevention (DLP) deployment
- Advanced threat detection with behavior analytics
- Security automation and orchestration

Requirement Selection Summary:

The following cryptographic controls were selected to address identified SSL/TLS vulnerabilities and ensure NIST compliance.

Total Requirements Selected: 47 individual security requirements across 8 major control categories

Selection Criteria Weighting:

- Mandatory Compliance (40%): NIST SP 800-53 requirements for government customers
- Critical Risk Mitigation (35%): Protection against identified Critical and High vulnerabilities
- Industry Best Practices (15%): CIS Benchmarks and ISO 27001 alignment
- Business Continuity (10%): Operational requirements with minimal service disruption

Key Decision Principle:

Every security requirement selected satisfied at least one of the following criteria:

- Addresses identified vulnerability (vulnerability-driven requirement)
- Meets compliance mandate (regulation-driven requirement)
- Protects crown jewel asset (risk-driven requirement)
- Prevents documented attack path (threat-driven requirement)

---

3. Implementation Methodology and Execution (IMPLEMENTED)

Technical implementation of the security requirements, including procedures, tools, configurations, and validation steps.

3.1 Implementation Framework and Governance

Project Change Request (PCR) Process:

All security changes followed Design World's formal change management process to ensure proper governance and approval.

PCR Components:

Change Summary: Description of specific technical modifications

Justification: Risk mitigation objectives and compliance alignment

Risk Assessment: Impact analysis with and without implementation approval

Implementation Plan: Detailed step-by-step technical procedures

Testing and Validation: Pre-production testing requirements

Rollback Procedures: Recovery plans if implementation fails

Approval Authority: CCB Chair, CTO, and Lead Security Engineer signatures required

Major PCRs Submitted and Approved:

1. PCR-001: Harden Domain Controller (172.16.1.205)

2. PCR-002: Harden File Server (172.16.1.138)

3. PCR-003: Harden User Workstations (172.16.1.41, 172.16.1.93)

4. PCR-004: Harden Linux Servers (172.16.1.62, 172.16.1.94, 172.16.1.183, 172.16.1.202)

Implementation Methodology:

The team followed NIST Cybersecurity Framework functions as implementation methodology:

Phase-Based Approach:

Phase 1: Emergency Containment (Days 1-3)

- Critical vulnerability remediation (MS17-010 patching, SMBv1 disablement)
- Immediate firewall rule implementation for AD port restriction
- Emergency patching deployment on critical systems

Phase 2: Tactical Hardening (Weeks 1-2)

- Protocol disablement (SMBv1 removal across environment)
- Cryptographic modernization (TLS enforcement, weak cipher removal)
- Access control enforcement (NLA activation, MFA deployment initiation)

Phase 3: Strategic Controls (Weeks 3-8)

- Monitoring infrastructure deployment (SIEM implementation)
- Configuration management system deployment
- Continuous vulnerability scanning establishment

Phase 4: Validation and Optimization (Weeks 8-10)

- Comprehensive security retesting via vulnerability scans
- Penetration testing to validate control effectiveness
- Performance optimization and fine-tuning
- Documentation completion for audit readiness

3.2 Domain Controller Hardening:

Asset: DW-DC-OL1 (172.16.1.205) - Windows Server 2016 Active Directory Domain Controller

SMBv1 Protocol Disablement:

SMBv1 was disabled to eliminate the MS17-010 (EternalBlue) vulnerability vector. The SMB1Protocol Windows feature was disabled via PowerShell, and registry modifications ensured complete removal of SMBv1 server and client components. Post-implementation verification confirmed EnableSMB1Protocol = False.

Critical Security Patching:

Microsoft security update KB4013389 (MS17-010) was applied along with supporting updates KB4012212 and KB4012213. Patch installation was verified via Get-HotFix command, and monthly security rollups were applied to establish the current patch baseline.

Active Directory Port Restrictions:

Windows Firewall rules were configured to restrict Active Directory service ports (389, 636, 88, 445, 135, 3268, 3269) to the management subnet (172.16.1.0/26) only. Default deny rules block all AD traffic from untrusted networks, preventing lateral movement from compromised systems.

Network Level Authentication (NLA):

NLA was enabled on the Domain Controller RDP service via registry modification (UserAuthentication = 1). This requires authentication before RDP session establishment, blocking pre-authentication exploits and brute-force attempts.

Multi-Factor Authentication (MFA):

Azure AD MFA was integrated with on-premises Active Directory using Conditional Access policies. Deployment followed phased rollout: IT administrators first, then security team, then all Domain Admins. MFA is now required for all privileged access to the Domain Controller.

SIEM Log Forwarding:

Windows Event Forwarding was configured to send critical security events to the SIEM collector. Monitored events include successful logons (4624), failed logons (4625), privilege assignments (4672), and Kerberos authentication (4768/4769).

3.3 File Server and Workstation Hardening:

File Server: DW-FS-OL1 (172.16.1.138)

TLS/SSL Configuration:

Deprecated protocols (TLS 1.0, TLS 1.1) and weak cipher suites (RC4, 3DES) were disabled via SCHANNEL registry configuration to address CVE-2016-2183 (SWEET32) and CVE-2013-2566 (Bar Mitzvah) vulnerabilities. Strong AES-GCM cipher suites with Perfect Forward Secrecy were enabled. Post-implementation SSL scanning confirmed only TLS 1.2/1.3 connections accepted with no weak ciphers available.

Certificate Replacement:

Self-signed certificates were replaced with CA-issued certificates using SHA-256 signatures. Certificate Signing Requests were generated with 2048-bit key length and submitted to the internal Active Directory Certificate Services CA. Signed certificates were imported and bound to RDP and file sharing services, enabling proper certificate chain validation for clients.

User Workstations: DW-WIN10-1 (172.16.1.93), DW-WIN10-2 (172.16.1.41)

RDP Service Disablement:

RDP was disabled on user workstations via registry modification (fDenyTSConnections = 1) to eliminate unnecessary attack surface. Windows Firewall rules for Remote Desktop were also disabled. Port scanning confirmed TCP/3389 closed on both workstations. Users access workstations via VPN and primary console only.

Host-Based Firewall:

Windows Firewall was enabled on all profiles (Domain, Public, Private) with default inbound action set to Block. Firewall logging was enabled to capture allowed and blocked traffic. Custom rules allow only required outbound traffic: HTTPS (443) for web access, DNS (53) for name resolution, and SMB (445) to file server IP (172.16.1.138) only.

3.4 Linux Server Hardening:

Assets: Ubuntu 20.04 LTS servers at 172.16.1.62, 172.16.1.94, 172.16.1.183, 172.16.1.202

Package Updates:

System updates applied via apt-get update && apt-get upgrade with --break-system-packages flag for pip installations. Kernel security patches verified via uname -r showing updated kernel versions. Iptables rules configured to drop ICMP timestamp requests (type 13) and timestamp replies (type 14) to prevent network reconnaissance: *iptables -A INPUT -p icmp --icmp-type timestamp-request -j DROP.*

UFW Firewall Deployment:

UFW default policy configured via ufw default deny incoming && ufw default allow outgoing. SSH access (port 22) explicitly permitted from management subnet only: ufw allow from 172.16.1.0/26 to any port 22. Firewall status verified via ufw status verbose confirming active ruleset with logging enabled for denied connections.

Unnecessary Services Disabled:

Service disablement executed via *systemctl* disable --now for each target service. Verification performed via *systemctl* status confirming inactive/dead status. Automatic security updates configured via unattended-upgrades package with Unattended-Upgrade::Allowed-Origins limited to security repositories only, preventing unexpected feature updates during production hours.

---

4. Validation and Testing Framework (TESTED)

This section documents validation and testing methodology used to confirm implemented security control effectiveness.

4.1 Post-Hardening Vulnerability Assessment:

Methodology:

Post-hardening vulnerability scanning was conducted using Tenable Nessus Professional with identical configuration to baseline assessment. Authenticated credentialed scans covered all eight in-scope systems.

Results Summary:

Vulnerability scanning confirmed complete remediation across all severity levels:

Figure 6 - Vulnerability Remediation Results

Critical	1 reduced to 0
High	5 reduced to 0
Medium	24 reduced to 0
Low	5 reduced to 0
Total	35 reduced to 0 (100% remediation)

CVE-Specific Validation:

- CVE-2017-0143, CVE-2017-0144, CVE-2017-0145 (MS17-010 EternalBlue family): Confirmed remediated on Domain Controller
- CVE-2016-2183 (SWEET32): Confirmed remediated across all affected hosts
- CVE-2013-2566, CVE-2015-2808 (RC4 Bar Mitzvah): Confirmed remediated across all affected hosts

Complete post-hardening vulnerability scan results are documented in Assignment 2.1 - Final Vulnerability Assessment Report, Appendix A. The appendix contains detailed Nessus scan screenshots for all eight in-scope systems, demonstrating zero critical, high, medium, and low severity vulnerabilities across the entire environment. Each host scan result includes the characteristic Nessus severity bar chart showing 0-0-0-0 across all vulnerability categories, with only informational findings related to system enumeration and service detection remaining. This comprehensive scan evidence validates the complete elimination of all 35 vulnerabilities identified during the baseline assessment and confirms the environment has achieved a secure, hardened baseline posture.

Figure 7 - Post-Hardning Vulnerability Status by Host

Affected Host	Critical	High	Medium	Low
172.16.1.41	0	0	0	0
172.16.1.62	0	0	0	0
172.16.1.93	0	0	0	0
172.16.1.94	0	0	0	0
172.16.1.138	0	0	0	0
172.16.1.183	0	0	0	0
172.16.1.202	0	0	0	0
172.16.1.205	0	0	0	0

4.2 Configuration Verification and Penetration Testing:

Manual Configuration Verification:

Configuration verification was performed to confirm all hardening measures were properly applied across the environment.

SMBv1 Verification:

PowerShell commands confirmed SMBv1 protocol disabled on Domain Controller (172.16.1.205) and File Server (172.16.1.138). Get-SmbServerConfiguration returned EnableSMB1Protocol = False on both systems.

TLS/SSL Verification:

SSL scanning confirmed only TLS 1.2/1.3 connections accepted. Connection attempts using TLS 1.0, TLS 1.1, RC4, and 3DES ciphers were all refused with "no shared cipher" errors.

Firewall Verification:

Windows Firewall confirmed enabled on all Windows systems with default deny inbound policy. UFW confirmed active on all Linux servers with deny incoming policy. Network testing confirmed expected traffic flows permitted while unauthorized connections blocked.

Post-Hardening Penetration Testing:

Penetration testing was conducted following NIST SP 800-115 methodology to validate that implemented controls prevent real-world exploitation attempts.

MS17-010 (EternalBlue) Exploitation:

Metasploit exploitation attempt against Domain Controller failed with "target does not appear vulnerable" result, confirming SMBv1 remediation effective

RDP Brute Force Attack:

Hydra brute force attack blocked by Network Level Authentication preventing pre-authentication attempts; account lockout policy triggered after 5 failed attempts

TLS Downgrade Attack:

OpenSSL connection attempts using deprecated protocols and weak ciphers refused, confirming cryptographic hardening effectiveness.

Lateral Movement via SMB:

Attempted SMB connections between network segments blocked by firewall rules, confirming network segmentation effective

Testing Summary:

All 12 tested attack vectors were successfully blocked. Zero successful exploitations achieved post-hardening, confirming all previously identified attack paths have been closed through implemented security controls.Complete penetration test methodology and results are documented in Assignment 3.1 Final Penetration Test Report.

4.3 Compliance Framework Validation:

NIST SP 800-53 Assessment:

Comprehensive control assessment validated alignment with NIST SP 800-53 Rev. 5 requirements for US government customer compliance.

- Access Control (AC): Account lockout policies, firewall rules, file permissions implemented
- Identification and Authentication (IA): Active Directory authentication, MFA for privileged accounts, NLA enforcement
- System and Communications Protection (SC): TLS 1.2/1.3 encryption, network segmentation, host-based firewalls
- System and Information Integrity (SI): Patch management, vulnerability remediation, malware protection
- Audit and Accountability (AU): Security event logging, SIEM integration

All assessed technical controls achieved compliance. Design World meets mandatory NIST SP 800-53 requirements for US government customer contracts.

CIS Benchmark Assessment:

- Systems were assessed against CIS Benchmark standards:
- Windows Server 2016 Benchmark: 176/178 controls passed (98.9%)
- Windows 10 Enterprise Benchmark: 198/201 controls passed (98.5%)
- Ubuntu Linux 20.04 LTS Benchmark: 154/156 controls passed (98.7%)
- Failed controls were low-risk informational items with documented business justification.

ISO 27001 Alignment:

Technical controls validated against ISO/IEC 27001:2013 Annex A requirements including Access Control (A.9), Cryptography (A.10), Operations Security (A.12), and Communications Security (A.13). All 40 assessed controls achieved compliance. Environment is prepared for formal ISO 27001 certification audit if required.

Compliance Attestation:

Design World's cybersecurity posture meets all mandatory compliance requirements for US government customers and satisfies applicable industry security frameworks.

---

5. Detailed Security Control Analysis

This section demonstrates end-to-end traceability for representative security controls, showing how requirements flowed from vulnerability discovery through implementation to validation. The following control examples illustrate the complete lifecycle documented in detail throughout Sections 2-4.

Control Example: SMBv1 Protocol Elimination

Why Chosen: CVE-2017-0143/0144/0145 (MS17-010) represented highest risk with CVSS 9.8 Critical severity. Active exploits including WannaCry and Petya ransomware provided direct path to Domain Controller compromise.

How Implemented: SMBv1 Windows feature disabled via PowerShell, MS17-010 security patch (KB4013389) applied, and WSUS configured to prevent re-enablement.

How Tested: Nessus scan confirmed CVEs no longer detected. Metasploit EternalBlue exploitation failed with "target not vulnerable" result. PowerShell verification confirmed EnableSMB1Protocol = False.

Compliance Mapping: NIST SP 800-53 SI-2, CIS Benchmark Section 18.3.8.1 - COMPLIANT

Control Example: TLS/SSL Modernization

Why Chosen: CVE-2016-2183 (SWEET32) and CVE-2013-2566 (RC4) exposed cryptographic weaknesses. US government customers require FIPS 140-2 compliant cryptography.

How Implemented: TLS 1.0/1.1 disabled, RC4 and 3DES cipher suites removed, AES-GCM cipher suites enabled, self-signed certificates replaced with CA-issued certificates.

How Tested: SSL scanning confirmed only TLS 1.2+ accepted. OpenSSL connection attempts with weak ciphers refused. SWEET32 attack simulation failed.

Compliance Mapping: NIST SP 800-53 SC-13, SC-12, CIS Benchmark Section 18.9.83 - COMPLIANT

Summary:

All security controls listed above were selected based on identified vulnerabilities and compliance requirements, implemented following formal change management procedures, and validated through vulnerability scanning and penetration testing. Detailed implementation procedures and test results are documented in Sections 3 and 4 respectively.

Figure 8 - Security Control Lifecycle Traceability Matrix

Control Category	**Requirement Driver**	**Implementation**	**Validation Result**
Vulnerability Management	CVE-2017-0143 (MS17-010	SMBv1 disabled	Patched, not detected in rescan
Cryptographic Protection	CVE-2016-2183 (SWEET32)	TLS 1.2 enforced	No weak ciphers available
Access Control	NIST IA-2(1)	MFA, NLA deployed	Brute force blocked
Network Security	NIST SC-7	Host firewalls enabled	Lateral movement blocked
Patch Management	NIST SI-2	Automated updates	Current patch levels verified

6. Compliance Framework Alignment

NIST SP 800-53 Comprehensive Mapping:

The following control family implementation summary demonstrates Design World's comprehensive compliance posture across all applicable NIST SP 800-53 control families:

Control family implementation summary:

- Access Control (AC): 25 applicable, 25 implemented (100%)
- Audit and Accountability (AU): 16 applicable, 16 implemented (100%)
- Awareness and Training (AT): 5 applicable, 4 implemented (80%)
- Configuration Management (CM): 14 applicable, 14 implemented (100%)
- Contingency Planning (CP): 8 applicable, 6 implemented (75%)
- Identification and Authentication (IA): 12 applicable, 12 implemented (100%)
- Incident Response (IR): 10 applicable, 8 implemented (80%)
- Maintenance (MA): 6 applicable, 6 implemented (100%)
- Media Protection (MP): 8 applicable, 7 implemented (87%)
- Physical and Environmental Protection (PE): 18 applicable, 15 implemented (83%)
- Planning (PL): 9 applicable, 9 implemented (100%)
- Personnel Security (PS): 8 applicable, 7 implemented (87%)
- Risk Assessment (RA): 10 applicable, 10 implemented (100%)
- System and Services Acquisition (SA): 12 applicable, 10 implemented (83%)
- System and Communications Protection (SC): 28 applicable, 28 implemented (100%)
- System and Information Integrity (SI): 23 applicable, 23 implemented (100%)

Total NIST SP 800-53 Controls:

- 212 applicable, 200 implemented (94.3% overall compliance)

100% compliance was achieved in all technical control families relevant to system hardening. Lower percentages in AT, CP, IR, PE, PS, and SA represent organizational controls outside the technical implementation project scope.

---

7. Organizational Impact and Risk Reduction

7.1 Quantitative Risk Reduction Analysis:

Pre-Hardening Risk Profile:

- Domain Controller (172.16.1.205): Critical Risk (CVSS 9.8) - SMBv1 vulnerabilities
- File Server (172.16.1.138): High Risk (CVSS 7.5) - Weak cryptographic configurations
- Workstations (172.16.1.41, 172.16.1.93): Medium Risk (CVSS 5.0) - Configuration weaknesses
- Linux Servers (172.16.1.62, .94, .183, .202): Medium Risk (CVSS 5.0) - Outdated packages

Environment Aggregate Risk: Critical: (CVSS 9.8)

Post-Hardening Risk Profile:

All systems reduced to Minimal Risk (0.0) with zero vulnerabilities detected across all severity levels.

Environment Aggregate Risk: Minimal: (CVSS 0.0) - representing 100% risk reduction

Risk Reduction Summary:

- Critical: 1 to 0 (100% elimination)
- High: 5 to 0 (100% elimination)
- Medium: 24 to 0 (100% elimination)
- Low: 5 to 0 (100% elimination)
- Total: 35 to 0 (100% reduction)

7.2 Business Impact Analysis:

Intellectual Property Protection:

- Design data secured through multi-layered defense-in-depth controls
- Domain compromise attack path eliminated through SMBv1 removal and AD hardening
- File exfiltration risk reduced through network segmentation and access controls

7.3 Regulatory and Compliance Impact:

- US Government Contracts: NIST SP 800-53 compliance validated, maintaining contract eligibility
- Cyber Insurance: Security controls adequate for policy coverage requirements
- Industry Standards: CIS Benchmark compliance (98%+) demonstrates security leadership

Operational Continuity:

- Ransomware Prevention: MS17-010 elimination prevents WannaCry-style attacks
- Business Downtime Prevention: Defensive controls enable continued operations
- Incident Response: SIEM monitoring enables rapid detection and response

7.4 Policy Governance and ISSP Framework:

To institutionalize security controls and ensure sustained compliance, Design World developed a formal Information System Security Policy (ISSP) governing all systems within the 172.16.1.0/24 network.

Key ISSP Policy Domains:

Access Control Policy: Multi-factor authentication required for administrative access; Network Level Authentication mandatory for RDP; principle of least privilege enforced via AD

Patch Management Policy: WSUS automatic patching for Windows (7-day approval cycle); unattended-upgrades for Linux; quarterly validation cycles

Cryptographic Standards Policy: TLS 1.2/1.3 mandatory; RC4 and 3DES prohibited; CA-issued certificates required

Network Security Policy: Active Directory services restricted to management subnet (172.16.1.0/26); host-based firewalls mandatory; VPN required for remote access

Monitoring and Audit Policy: SIEM integration for security events (4624, 4625, 4672, 4768/4769); 90-day log retention; monthly security reviews

Incident Response Policy: Defined escalation procedures; quarterly tabletop exercises; integrated organizational response framework

Compliance Alignment:

The ISSP operationalizes NIST SP 800-53, CIS Benchmarks (98%+ compliance), and ISO 27001 controls, ensuring maintained security posture through policy-driven governance and providing auditable evidence for regulatory requirements and customer contractual obligations.

---

8. Lessons Learned and Recommendations

Project Successes:

What Worked Well:

1. Risk-Driven Prioritization: Focusing on Critical and High vulnerabilities first (Domain Controller exposure) delivered immediate risk reduction and stakeholder confidence
2. Framework-Based Approach: NIST SP 800-53 provided clear requirements, CIS Benchmarks provided technical implementation guidance
3. Phased Implementation: Four-phase rollout enabled testing and validation at each stage with minimal business disruption
4. Change Management Process: Formal PCR process ensured stakeholder approval and comprehensive documentation
5. Multi-Layer Validation: Vulnerability scanning, penetration testing, and configuration verification provided confidence in control effectiveness

Challenges Encountered and Resolutions:

Challenge: Certificate Authority Infrastructure Deployment

Issue: Design World lacked internal PKI infrastructure for certificate issuance

Impact: Delayed TLS/SSL modernization by one week

Resolution: Deployed Active Directory Certificate Services as Domain CA with automated certificate enrollment

Lesson: Infrastructure dependencies should be identified during requirements phase planning

Challenge: Automated Patch Management Configuration

Issue: Initial unattended-upgrades configuration caused unplanned kernel update and system reboot during business hours

Impact: Brief service disruption on one application server (12 minutes downtime)

Resolution: Configured unattended-upgrades for download only with manual installation during approved maintenance windows

Lesson: Automation must include safeguards to prevent unexpected service disruptions

Recommendations for Future Enhancement:

Short-Term (0-6 months):

- Zero Trust Architecture Expansion: Deploy application-layer micro-segmentation
- Endpoint Detection and Response (EDR): Implement behavioral threat detection controls
- Security Awareness Training: Establish quarterly training program for all employees

Medium-Term (6-12 months):

- Privileged Access Management (PAM): Implement just-in-time privilege elevation
- Data Loss Prevention (DLP): Deploy monitoring for intellectual property exfiltration
- Backup and Disaster Recovery Testing: Quarterly restoration validation exercises

Long-Term (12-24 months):

- ISO 27001 Certification: Complete formal third-party certification audit
- Threat Intelligence Integration: Subscribe to industry threat intelligence feeds
- Red Team Exercises: Annual third-party adversarial assessment

---

9. Conclusion

Project Summary:

Design World's cybersecurity hardening project successfully transformed the organization's security posture from critically vulnerable to secure and compliant. Over a 10-week implementation period, CyberRealm Sentinel's Security Engineering Team systematically addressed all identified vulnerabilities through structured technical remediation and validation.

Achievement Summary:

- 100% Vulnerability Remediation: Eliminated all 35 identified vulnerabilities across Critical, High, Medium, and Low severity levels, confirmed through post-hardening vulnerability scanning.
- Zero Exploitable Attack Vectors: Post-hardening penetration testing confirmed no successful exploitation paths remain, with all tested attack vectors blocked by implemented controls.
- Full Compliance Achievement: Validated alignment with NIST SP 800-53 (100% of assessed technical controls), CIS Benchmarks (98%+ across platforms), and ISO 27001 standards.
- Requirements Lifecycle Demonstration: Complete traceability demonstrated from vulnerability discovery (requirements chosen based on risk) through technical implementation (security controls deployed and configured) to validation (multi-layer testing confirming effectiveness).
- Regulatory Compliance: Met mandatory NIST SP 800-53 requirements for US government customer contracts, ensuring continued contract eligibility and business operations.

Organizational Transformation:

The security program extends beyond technical controls to establish sustainable security operations. Through implementation of structured processes, continuous monitoring capabilities, and compliance frameworks, Design World had transitioned from a reactive security posture to a proactive, resilient model. This transformation ensures that security is no longer a one-time project but an ongoing operational capability integrated into daily business functions.

Operational Security Program Established:

- 30-day critical patch SLA implemented and maintained
- Monthly vulnerability scanning with automated tracking
- SIEM-enabled continuous security monitoring operational

Compliance Posture Achieved:

- NIST SP 800-53 compliance validated for government customers
- CIS Benchmark compliance (98%+) established
- ISO 27001 certification readiness confirmed

Business Value Delivered:

- Intellectual property protection through multi-layered security controls
- Government contract eligibility maintained through NIST compliance
- Cyber insurance policy requirements satisfied

Final Assessment:

Design World successfully addressed critical security challenges through systematic vulnerability remediation and security control implementation. The journey from 35 vulnerabilities to zero, and from critical risk to minimal risk, establishes a secure and compliant operational foundation supporting Design World's continued business success.

Moving forward, Design World has established a technically secure infrastructure supported by comprehensive policy governance through the ISSP framework. The combination of technical controls, validated compliance, and continuous monitoring provides sustainable protection for intellectual property while satisfying regulatory requirements across all three global locations. This transformation represents a fundamental shift from reactive incident response to proactive, policy-driven risk management—positioning Design World to confidently serve US government customers and protect its most valuable assets in an evolving threat landscape.

---

10. Appendices

Appendix A: System Inventory

Complete Asset Inventory with Technical Specifications

DW-DC-OL1 (172.16.1.205):

Operating System: Windows Server 2016

Role: Active Directory Domain Controller (Primary)

vCPU: 16, RAM: 16GB, Storage: 200GB

Status: In-Scope for hardening

DW-FS-OL1 (172.16.1.138):

Operating System: Windows Server 2016

Role: File Server (Design IP Storage)

vCPU: 16, RAM: 16GB, Storage: 200GB

Status: In-Scope for hardening

DW-WIN10-1 (172.16.1.93):

Operating System: Windows 10 Pro

Role: User Workstation (Design Applications)

vCPU: 4, RAM: 16GB, Storage: 200GB

Status: In-Scope for hardening

DW-WIN10-2 (172.16.1.41):

Operating System: Windows 10 Pro

Role: User Workstation (Engineering Applications)

vCPU: 4, RAM: 16GB, Storage: 200GB

Status: In-Scope for hardening

DW-UBUNTU-1 (172.16.1.183):

Operating System: Ubuntu 20.04 LTS

Role: Linux Server (General Purpose)

vCPU: 4, RAM: 16GB, Storage: 200GB

Status: In-Scope for hardening

DW-UBUNTU-2 (172.16.1.202):

Operating System: Ubuntu 20.04 LTS

Role: Linux Server (General Purpose)

vCPU: 4, RAM: 16GB, Storage: 200GB

Status: In-Scope for hardening

DW-UBUNTU-3 (172.16.1.94):

Operating System: Ubuntu 20.04 LTS

Role: Linux Server (General Purpose)

vCPU: 4, RAM: 16GB, Storage: 200GB

Status: In-Scope for hardening

DW-UBUNTU-4 (172.16.1.62):

Operating System: Ubuntu 20.04 LTS

Role: Linux Server (General Purpose)

vCPU: 4, RAM: 16GB, Storage: 200GB

Status: In-Scope for hardening

Network Infrastructure:

Primary Network: 172.16.1.0/24

DHCP Pool: 172.16.10.0/24

Management Subnet: 172.16.1.0/26 (restricted administrative access)

VPN Gateway: Cloud provider managed gateway

Appendix B: Vulnerability Details

Initial Vulnerability Findings - Detailed Breakdown

Critical Severity (CVSS greater than or equal to 9.0):

CVE-2017-0143 – MS17-010 SMBv1 Remote Code Execution (EternalBlue)

CVSS: 9.8

Affected Host: 172.16.1.205

Exploit Availability: Yes (Metasploit module available)

CVE-2017-0144 – MS17-010 SMBv1 Remote Code Execution (EternalChampion)

CVSS: 9.8

Affected Host: 172.16.1.205

Exploit Availability: Yes (Metasploit module available)

CVE-2017-0145 – MS17-010 SMBv1 Remote Code Execution (EternalRomance)

CVSS: 9.8

Affected Host: 172.16.1.205

Exploit Availability: Yes (Metasploit module available)

High Severity (CVSS 7.0-8.9):

CVE-2016-2183 – SWEET32 3DES Cipher Suite Vulnerability

CVSS: 7.5

Affected Hosts: 172.16.1.205, 172.16.1.138, 172.16.1.41, 172.16.1.93

Exploit Availability: Yes (cryptographic weakness exploitation)

Medium Severity (CVSS 4.0-6.9):

CVE-2013-2566 – RC4 Cipher Suites Enabled (Bar Mitzvah)

CVSS: 5.9

Affected Hosts: 172.16.1.205, 172.16.1.138

CVE-2015-2808 – RC4 Cipher Suites Enabled (Bar Mitzvah)

CVSS: 5.9

Affected Hosts: 172.16.1.205, 172.16.1.138

Additional Medium/Low Vulnerabilities:

Missing Windows security updates and Ubuntu package vulnerabilities across multiple hosts (CVSS 4.0-6.9 range).

---

11. Glossary of Terms

Active Directory (AD)	Microsoft directory service for centralized authentication and authorization in Windows domains.
AES-GCM	Advanced Encryption Standard in Galois/Counter Mode, strong symmetric encryption cipher providing both confidentiality and authentication.
CIS Benchmark	Center for Internet Security configuration baseline standards providing prescriptive security guidance.
CVSS	Common Vulnerability Scoring System, standardized method for rating vulnerability severity from 0.0 to 10.0.
Data Loss Prevention (DLP)	Security technologies that detect and prevent unauthorized transmission of sensitive data outside organizational boundaries.
Endpoint Detection and Response (EDR)	Security solution that continuously monitors endpoints (workstations, servers) for malicious activity and provides threat detection, investigation, and response capabilities.
EternalBlue	NSA-developed exploit targeting SMBv1 vulnerability (CVE-2017-0143/0144/0145), used by WannaCry and Petya ransomware.

FIPS 140-2	Federal Information Processing Standard for cryptographic module validation required for US government systems.
ISO 27001	International Organization for Standardization information security management system (ISMS) standard providing framework for protecting organizational information assets.
MFA	Multi-Factor Authentication, security mechanism requiring two or more verification factors for authentication.
MS17-010	Microsoft Security Bulletin for SMBv1 vulnerabilities released March 2017, addressed by KB4013389 patch.
NLA	Network Level Authentication, RDP security feature requiring authentication before session establishment to prevent pre-authentication attacks.
NIST SP 800-53	US National Institute of Standards and Technology security and privacy control framework for federal information systems.
Privileged Access Management (PAM)	Security solution controlling and monitoring privileged user access to critical systems, implementing just-in-time elevation and session recording.
PCR	PCR: Project Change Request, formal documentation requesting approval for system configuration changes.

Perfect Forward Secrecy (PFS)	Cryptographic property ensures session key compromise does not expose past communication sessions.
RC4	Rivest Cipher 4, deprecated stream cipher with known cryptographic vulnerabilities.
SIEM	Security Information and Event Management, centralized platform for log collection, analysis, and security alerting.
SMBv1	Server Message Block version 1, legacy file sharing protocol with critical remote code execution vulnerabilities.
SWEET32	Cryptographic attack against 64-bit block ciphers including 3DES and Blowfish.
TLS	Transport Layer Security, cryptographic protocol providing secure network communications.
UFW	UFW stands for "Uncomplicated Firewall" - it's the Ubuntu Linux firewall tool you reference throughout Section 3.4. VPN (Virtual Private Network) is a completely different technology.
Zero Trust Architecture	Security model that requires strict identity verification for every user and device attempting to access resources, regardless of network location.

12. References

Primary Standards and Frameworks:

1. National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53, Rev. 5). U.S. Department of Commerce.

2. National Institute of Standards and Technology. (2016). Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (NIST Special Publication 800-160, Vol. 1). U.S. Department of Commerce.

3. National Institute of Standards and Technology. (2008). Technical Guide to Information Security Testing and Assessment (NIST Special Publication 800-115). U.S. Department of Commerce.

4. Center for Internet Security. (2021). CIS Microsoft Windows Server 2016 Benchmark v1.4.0. CIS Benchmarks.

5. Center for Internet Security. (2021). CIS Ubuntu Linux 20.04 LTS Benchmark v1.1.0. CIS Benchmarks.

6. International Organization for Standardization. (2013). Information Technology - Security Techniques - Information Security Management Systems - Requirements (ISO/IEC 27001:2013).

Vulnerability References:

7. Microsoft Corporation. (2017). Microsoft Security Bulletin MS17-010 - Critical: Security Update for Microsoft Windows SMB Server (4013389). Microsoft Security Response Center.
8. MITRE Corporation. (2017). CVE-2017-0143: Microsoft Windows SMB Remote Code Execution Vulnerability. Common Vulnerabilities and Exposures Database.

9. MITRE Corporation. (2016). CVE-2016-2183: The DES and Triple DES Ciphers, as Used in the TLS, SSH, and IPSec Protocols (SWEET32 Attack). Common Vulnerabilities and Exposures Database.

Project-Specific Documentation:

10. Design World. (2024, September 2). Design World Case Study Requirements. University of San Diego.
11. CyberRealm Sentinels. (2025, October 3). Final Vulnerability Assessment Report for Design World (Assignment 2.1). University of San Diego.
12. CyberRealm Sentinels. (2025, October 3). Final Penetration Test Report for Design World (Assignment 3.1). University of San Diego.
13. CyberRealm Sentinels. (2025, October 6). Security Hardening Plan and Project Change Request (PCR) for Design World (Assignment 5.1). University of San Diego.
14. CyberRealm Sentinels. (2025, October 20). Security Hardening Report with Updated System Design and Drawings for Design World (Assignment 7.1). University of San Diego.

Document Control:

Document Information:

- Title: Design World Project Report - How Security Requirements Were Chosen, Implemented, and Tested
- Version: 1.0 (Final)
- Date: November 24, 2025
- Classification: Academic Project Submission
- Author: CyberRealm Sentinels Security Engineering Team (Kayvon)
- Course: CYBR-516 Capstone Project
- Institution: University of San Diego

END OF REPORT

This comprehensive report documents the complete lifecycle of Design World's cybersecurity hardening program from vulnerability assessment through implementation and validation. All security controls described have been implemented, tested, and validated as effective as of November 24, 2025.
