

# **Security Hardening Report with Updated System Design and Drawings**

**For:** Design World (DW)

**Prepared by:** CyberRealm Sentinels

**Date:** 10/20/25



## **CyberRealm Sentinels - Guardians of Partnered Firms**



## **Security Hardening Report with Updated System Design and Drawings for Design World**

**10/20/25**

Security Hardening Report with Updated System Design and Drawings

For: Design World (DW)

Prepared by: CyberRealm Sentinels

Date: 10/20/25



Table of Contents

- 1. Executive Summary..... 1
  - Purpose.....1
  - Business Impact .....1
  - Summary of Key Risks Identified.....2
  - Summary Scope of Hardening (Systems & Applications).....2
  - Methodology .....2
  - Summary of Improvements.....3
  - Executive Takeaway — Security Hardening at Design World .....7
  - Deliverable .....7

The Security Hardening Report with Updated System Design and Drawings

- 1. Introduction.....8
- 2. Purpose of Security Hardening .....9
- 3. Objectives of Security Hardening .....10
- 4. Assessment Scope .....12
- 5. Key Risks Identified.....14
- 6. Detailed Scope of Hardening (Systems & Applications).....15
- 7. Mitigation plan for outstanding issues and risk .....16
- 8. Hardening the System - Detailed Improvements (Systems & Applications) .....18
- 9. Tested Exploitable Vulnerabilities and Status .....33
- 10. Validation and Acceptance Criteria .....36

**Security Hardening Report with Updated System Design and Drawings**

**For:** Design World (DW)

**Prepared by:** CyberRealm Sentinels

**Date:** 10/20/25



11. Recommended Security Architecture for Design World .....42

12. Conclusion.....44

13. Next Steps.....44

14. Appendix A - Evidence (uploaded detailed Nessus rescan files) .....45

15. Appendix B - Glossary of Terms.....54

16. References.....55

# Security Hardening Report with Updated System Design and Drawings

**For:** Design World (DW)

**Prepared by:** CyberRealm Sentinels

**Date:** 10/20/25



## **1. Executive Summary**

Design World made significant progress by centralizing its operations and strengthening data protection upon transitioning to a private enterprise cloud. The critical security exposures revealed during the firm's most recent infrastructure penetration test and vulnerability assessment pose a significant risk to its intellectual property, operations, and client trust.

### **Purpose**

Immediate remediation is required to safeguard Design World's most valuable asset—its innovative designs. This report aims to detail the immediate and ongoing remediation actions and efforts taken to secure Design World's core assets, primarily its innovative design data and associated infrastructure against advanced threats.

### **Business Impact**

Not hardening Design World's systems risks catastrophic IP theft, financial losses, reputational collapse, and regulatory penalties. For a design firm whose value lies in its creativity and engineering innovation, failing to secure systems is equivalent to leaving the company's crown jewels unguarded. If left unaddressed, these vulnerabilities could enable attackers to gain domain-wide control, exfiltrate sensitive design assets, deploy ransomware, and disrupt operations. The reputational and regulatory consequences would be severe.

# Security Hardening Report with Updated System Design and Drawings

**For:** Design World (DW)

**Prepared by:** CyberRealm Sentinels

**Date:** 10/20/25



## Summary of Key Risks Identified

- Critical exposure of the Domain Controller (172.16.1.205)
- Exploitable SMBv1 vulnerabilities (EternalBlue family)
- Widespread RDP exposure
- Weak SSL/TLS configurations
- Patching and configuration gaps

## Summary Scope of Hardening (Systems & Applications)

The hardening effort applies to all core servers that support Design World's private enterprise cloud and remote workforce. The scope includes:

- Server Operating Systems and associated technology stacks.

## Methodology

Our hardening and validation approach leverages the NIST Cybersecurity Framework functions (Identify/Protect/Detect/Respond/Recover), NIST SP 800-160 for systems security engineering, NIST SP 800-53 Rev. 5 control families for requirements mapping, CIS Benchmarks (Windows Server 2016 and Windows 10) for configuration baselines, and NIST SP 800-115/PTES techniques for verification and re-testing (NIST SP 800-160; NIST SP 800-53 Rev. 5; NIST SP 800-115; CIS Benchmarks).



## Summary of Improvements

1. Disabled Remote Desktop (RDP) on DW-WIN10-01 and DW-WIN10-02 (Windows 10).

Disabling RDP on DW-WIN10-01 and DW-WIN10-02 removes a high-risk remote access channel, ensuring that all remote administration and user access flows through controlled, monitored, and MFA-protected paths. This significantly lowers the likelihood of credential compromise, ransomware deployment, or domain escalation via these endpoints.

2. Disabled Remote Desktop (RDP) on DW-FS-OL1 and DW-DC-OL1 (Windows Server 2016).

Disabling Remote Desktop Protocol (RDP) on DW-FS-OL1 (File Server) and DW-DC-OL1 (Domain Controller) both running Windows Server 2016 is a critical hardening step with very specific security benefits.

Disabling RDP on DW-FS-OL1 and DW-DC-OL1 removes a high-risk remote access channel from two of the most sensitive servers in the enterprise. It forces all administrative access through secure, monitored, MFA-enforced jump hosts, dramatically reducing the likelihood of domain compromise, ransomware deployment, or IP theft.



3. Updated the packages on all Ubuntu machines
  - Installed iptables and configured rules to block and silently discard ICMP timestamp request packets that are sent *to the host*.
  - By blocking ICMP timestamp requests, Design World has closed off a subtle but exploitable reconnaissance channel, making its systems harder to detect, fingerprint, and target — without affecting legitimate business operations.
4. SMBv1 disabled on DW-DC-OL1
  - Disabling SMBv1 on DW-DC-OL1 means Design World successfully shut down a legacy backdoor that attackers have used worldwide to cripple organizations. It forces all communication onto secure, modern protocols and dramatically reduces the chance of catastrophic domain compromise.
5. Enabled host-based firewall (UFW) on Ubuntu machines
  - Enabled host-based firewall (UFW) on Ubuntu, to meet Linux hardening standards for 172.16.1.202.
  - By enabling UFW on Ubuntu machines, Design World ensures that every server enforces its own security perimeter, reducing attack surface, blocking lateral movement, and aligning with Zero Trust principles, without disrupting legitimate operations.



6. Disabled Avahi, CUPS, CUPS-browsed, and Bluetooth services on Ubuntu host

172.16.1.202.

- Disabled Avahi, CUPS, CUPS-browsed, and Bluetooth services to reduce unnecessary network broadcasts, printer sharing, and wireless pairing exposure on Ubuntu host 172.16.1.202.

7. Enabled Windows SmartScreen to warn before running unrecognized systems from “Don’t” to “Warn”

- Enabling Windows SmartScreen from “Don’t do anything” to “Warn” on Design World’s systems is a preventive hardening control that directly strengthens endpoint protection and user behavior.
- Enabling SmartScreen warnings transforms every Design World workstation into a more cautious gatekeeper thereby stopping unrecognized or malicious software before it can run, and reducing the risk of human error leading to a breach.

8. Enabled network level authentication (NLA) for remote Desktop

- Used powershell to enable network level authentication (NLA) for remote Desktop. This change enforces verification before an RDP session starts, reducing the risk of unauthorized access.





## 9. Enabled the Windows Firewall

- Used Powershell to enable the Windows Firewall across all profiles using *netsh advfirewall* set all profiles state on.
- Enabling Windows Firewalls ensures that every workstation and server enforces its own traffic rules, blocking unauthorized access, preventing lateral movement, and aligning with Zero Trust principles — all without disrupting legitimate business operations.

## 10. Verified the disablement of MBv1 protocol on DW-FS-OL1 and DW-DC-OL1 (Windows Server 2016).

- Verifying that SMBv1 is disabled on DW-FS-OL1 and DW-DC-OL1 proves that Design World has eliminated a legacy backdoor exploited in some of the most damaging cyberattacks in history. At the system level, it forces all traffic onto secure, modern protocols; at the organizational level, it demonstrates risk reduction, compliance alignment, and a visible commitment to protecting intellectual property and business continuity.

## 11. Verified package updates on Ubuntu 172.16.1.202.

- Verifying package updates on Ubuntu hosts proves that Design World has closed known vulnerabilities on the hosts, established a secure baseline, and demonstrated disciplined patch management. At the system level, it



reduces the risk of exploitation; at the organizational level, it signals resilience, compliance, and a proactive security culture.

## 12. SSL/TLS Configuration Modernization

- Implemented SSL/TLS Configuration Modernization to address Weak SSL/TLS configurations.
- Deprecated ciphers (RC4, SWEET32) removed.
- Implemented TLS 1.2 and 1.3 where applicable.
- Applied strong cipher suites such as AES-GCM with forward secrecy.

## 13. Patch Management and Configuration

- Implemented Patch Management and Configuration to address patching and configuration gaps.
- Established consistent patch management practices to ensure all Windows and Linux hosts stay current.
- Automated vulnerability scanning to detect missing patches.

## Executive Takeaway — Security Hardening at Design World

The hardening exercise has moved Design World from a vulnerable, post-breach posture to a resilient, security-mature enterprise. All earlier identified vulnerabilities are hereby remediated.

## Deliverable

Security Hardening Report with updated system design and drawings (as Required).



## **The Security Hardening Report with Updated System Design and Drawings**

### **1. Introduction**

Following the firm's most recent infrastructure penetration test and vulnerability assessment, Design World's highest risks were: (a) Active Directory exposure on the domain controller (172.16.1.205) with legacy SMBv1, (b) broad RDP availability without enforced NLA/MFA, (c) deprecated cipher suites (RC4/3DES/SWEET32), and (d) patch discipline gaps.

We implemented a targeted hardening program and validated outcomes with authenticated scans and configuration evidence. Key results include, among others: SMBv1 disabled on Windows DC; disabled Remote Desktop (RDP) on DW-FS-OL1 and DW-DC-OL1 (Windows Server 2016); disabled Remote Desktop (RDP) on DW-DW-WIN10-01 and DW-WIN10-02 (Windows 10); enabled the Windows Firewall; all Ubuntu machines' packages updated; etc. Updated diagrams reflect network segmentation and least-privilege admin flows.



## **2. Purpose of Security Hardening**

This can be seen as follows:

### **a) Immediate Purpose:**

Contain and remediate the critical vulnerabilities (EternalBlue, SWEET32, RC4, exposed RDP services) that directly threaten Design World's domain controller and design data.

### **b) Strategic Purpose:**

Build a resilient, future-proof security posture that:

- Safeguards Design World's reputation and client trust.
- Supports business growth without introducing unmanaged risk.
- Provides executives with confidence that Intellectual Property (IP) is protected and operations are stable.

### **c) Long-Term Purpose:**

Transition Design World from a reactive, post-breach posture to a proactive, Zero Trust model with continuous monitoring, segmentation, and governance.



### **3. Objectives of Security Hardening for Design World (DW)**

#### **1. Protect Intellectual Property (IP)**

- Design World's competitive advantage lies in its artistic structural support designs. Hardening ensures that sensitive design files, models, and engineering data are shielded from theft or tampering.

#### **2. Reduce Attack Surface**

- By disabling unnecessary services (e.g., SMBv1), restricting RDP, and enforcing modern encryption, Design World minimizes the number of exploitable entry points for adversaries.

#### **3. Ensure Compliance & Governance**

- Align with recognized frameworks (NIST SP 800-53, ISO/IEC 27001) to demonstrate due diligence, satisfy client/regulatory expectations, and prepare for future audits.

#### **4. Strengthening Identity & Access Controls**

- Harden Active Directory, enforce MFA, and implement least-privilege access to prevent credential abuse and lateral movement.

#### **5. Improve Detection & Response**

- Enhance SIEM/IDS/IPS logging and monitoring so that attempted breaches are detected early, reducing dwell time and potential damage.

# **Security Hardening Report with Updated System Design and Drawings**

**For:** Design World (DW)

**Prepared by:** CyberRealm Sentinels

**Date:** 10/20/25



## **6. Establish a Secure Baseline**

- Create a hardened “gold image” for VMs and servers, ensuring consistency across regions (San Diego, Brussels, Hong Kong) and preventing configuration drift.

## **7. Enable Resilient Remote Collaboration**

- With 100% of employees remote, hardening ensures secure VPN access, encrypted communications, and safe collaboration across global teams.



#### 4. Assessment Scope

The assessment scope is shown in the figure below:

Figure 1 - In-Scope Systems

| <b>Instance Name</b>                           | <b>Operating System</b> | <b>Role/Function</b>               | <b>Resources</b>                | <b>Scope Status</b> |
|--|-------------------------|------------------------------------|---------------------------------|---------------------|
| Design-World-FA25-OL-1-<br>WindowsServer2016-1 | Windows<br>Server 2016  | Domain Controller<br>/ Core Server | 16 vCPUs,<br>200GB, 16GB<br>RAM | In-Scope            |
| Design-World-FA25-OL-1-<br>WindowsServer2016-2 | Windows<br>Server 2016  | Domain Controller<br>/ Core Server | 16 vCPUs,<br>200GB, 16GB<br>RAM | In-Scope            |
| Design-World-FA25-OL-1-<br>Win10Pro-1          | Windows 10<br>Pro       | User Workstation                   | 4 vCPUs,<br>200GB, 16GB<br>RAM  | In-Scope            |

## Security Hardening Report with Updated System Design and Drawings

**For:** Design World (DW)

**Prepared by:** CyberRealm Sentinels

**Date:** 10/20/25



|                                   |                |                                   |                                |          |
|-----------------------------------|----------------|-----------------------------------|--------------------------------|----------|
| Design-World-FA25-OL-1-Win10Pro-2 | Windows 10 Pro | User Workstation                  | 4 vCPUs,<br>200GB, 16GB<br>RAM | In-Scope |
| Design-World-FA25-OL-1-Ubuntu-1   | Ubuntu         | Linux Server<br>(general-purpose) | 4 vCPUs,<br>200GB, 16GB<br>RAM | In-Scope |
| Design-World-FA25-OL-1-Ubuntu-2   | Ubuntu         | Linux Server<br>(general-purpose) | 4 vCPUs,<br>200GB, 16GB<br>RAM | In-Scope |
| Design-World-FA25-OL-1-Ubuntu-3   | Ubuntu         | Linux Server<br>(general-purpose) | 4 vCPUs,<br>200GB, 16GB<br>RAM | In-Scope |
| Design-World-FA25-OL-1-Ubuntu-4   | Ubuntu         | Linux Server<br>(general-purpose) | 4 vCPUs,<br>200GB, 16GB<br>RAM | In-Scope |





## 5. Key Risks Identified

- **Critical exposure of the Domain Controller (172.16.1.205):** Active Directory services including (LDAP, Kerberos, SMB) protocols are accessible from untrusted networks, heightening the risk of full domain compromise and lateral movement by adversaries.
- **Exploitable SMBv1 vulnerabilities (EternalBlue family):** High-to-critical severity flaws (CVSS 8.1–9.8) capable of enabling remote code execution and ransomware propagation.
- **Widespread RDP exposure:** Multiple hosts with open RDP ports, lacking MFA and Network Level Authentication (NLA), increasing the risk of brute force and lateral movement.
- **Weak SSL/TLS configurations:** Use of deprecated cipher suites (RC4, SWEET32) that could allow interception and decryption of sensitive communications.
- **Patching and configuration gaps:** Outdated Windows builds and inconsistent patch management practices.



## 6. Detailed Scope of Hardening (Systems & Applications)

The hardening effort applies to all core infrastructure, endpoints, and applications that support Design World's private enterprise cloud and remote workforce. The scope includes:

### 1. Infrastructure Systems

- **Domain Controllers (DCs)** are particularly critical, with the host 172.16.1.205 running Active Directory (AD), DNS, LDAP, Kerberos, SMB, and RDP.
- **File Server**
- **Linux Infrastructure includes Apache server.**

### 2. Server Applications

- **Active Directory (AD):** Authentication, authorization, and identity management.
- **DNS, LDAP, Kerberos:** Core AD services exposed on DCs.
- **SMB/CIFS Services:** File sharing protocols (with SMBv1 disabled).
- **Remote Desktop Services (RDP):** Used for remote administration and user access to VMs.
- **Backup & Recovery Systems:** Cloud-based backup services and storage.

### 3. Endpoint Systems

- **Windows 10/11 Workstations:** Employee laptops/desktops (e.g., 172.16.1.41, 172.16.1.93).
- **Windows Server Instances:** File servers, application servers (e.g., 172.16.1.138).
- **Linux VMs:** Used for engineering/design workloads.



## 4. Network & Security Services

- **TLS/SSL Services:** Certificates and cipher configurations for VPN, RDP, and web-based services.
- **Firewall & Network Segmentation:** Rulesets controlling access to AD, RDP, and inter-site communication.
- **Logging & Monitoring Systems (SIEM):** Centralized log collection and anomaly detection.

## 5. User-Facing Applications

- **Design & Engineering Tools:** CAD/structural design applications hosted in the cloud VMs.
- **Business Applications:** Marketing and management tools accessed via VMs.
- **Collaboration Tools:** Zoom (for meetings), email, and file-sharing platforms (restricted to approved channels).

## 7. Mitigation plan for outstanding issues and risk

- 6.1 Critical exposures (0–72 hours)
- 6.2 High-risk vulnerabilities (3–14 days)
- 6.3 Medium-term controls (2–8 weeks)
- 6.4 Long-term resilience (2–6 months)

# **Security Hardening Report with Updated System Design and Drawings**

**For:** Design World (DW)

**Prepared by:** CyberRealm Sentinels

**Date:** 10/20/25



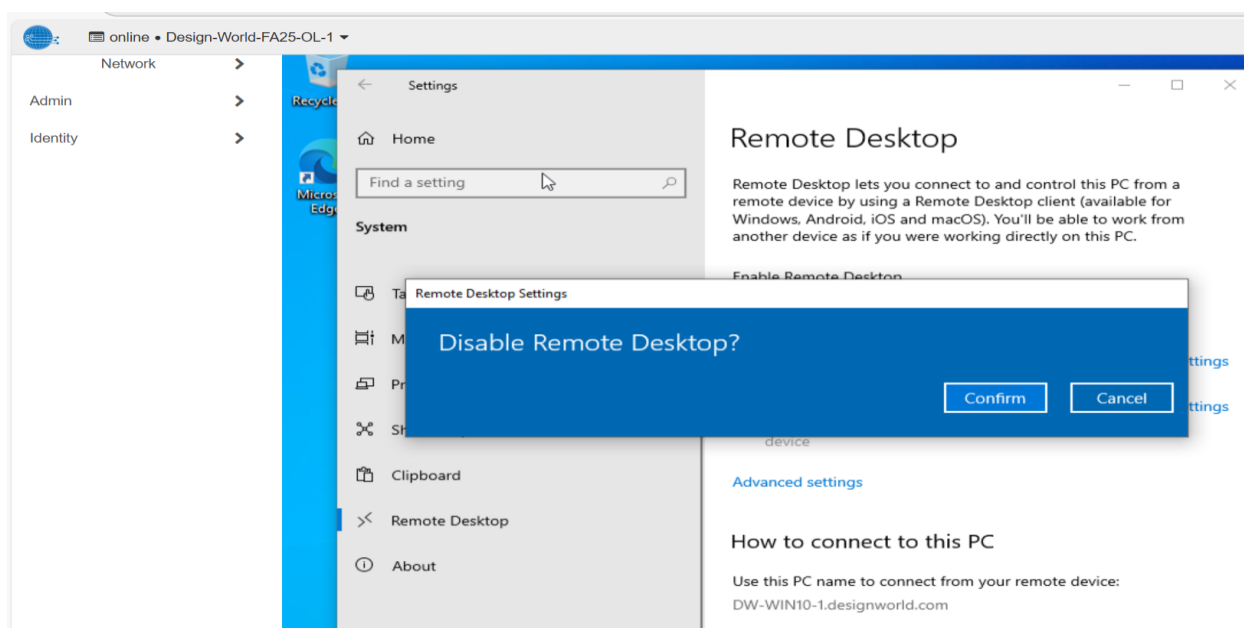
## 8. Hardening the System - Detailed Improvements (Systems & Applications)

The following actions were taken as follows and the resultant results were recorded:

### i) DW-WIN10-01 and DW-WIN10-02 (Windows 10):

- Disabled Remote Desktop (RDP) on DW-WIN10-01 and DW-WIN10-02 (Windows 10)

Figure 2 - Disabled Remote Desktop (RDP)



### Achievement

Disabling RDP on DW-WIN10-01 and DW-WIN10-02 removed a high-risk remote access channel, ensuring that all remote administration and user access flows through controlled, monitored, and MFA-protected paths. This significantly lowers the likelihood of credential compromise, ransomware deployment, or domain escalation via these endpoints.



ii) DW-FS-OL1 and DW-DC-OL1 (Windows Server 2016):

- Disabled Remote Desktop (RDP) on the above two,

Figure 3 - Pre - Disabled Remote Desktop

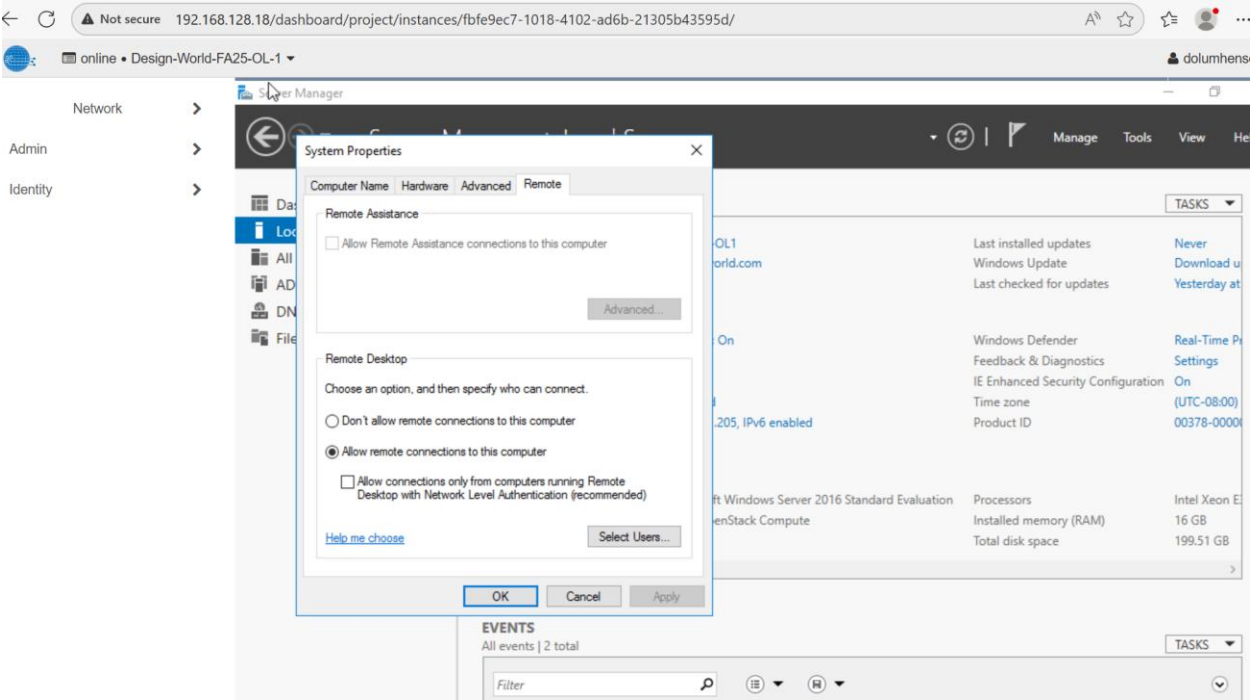
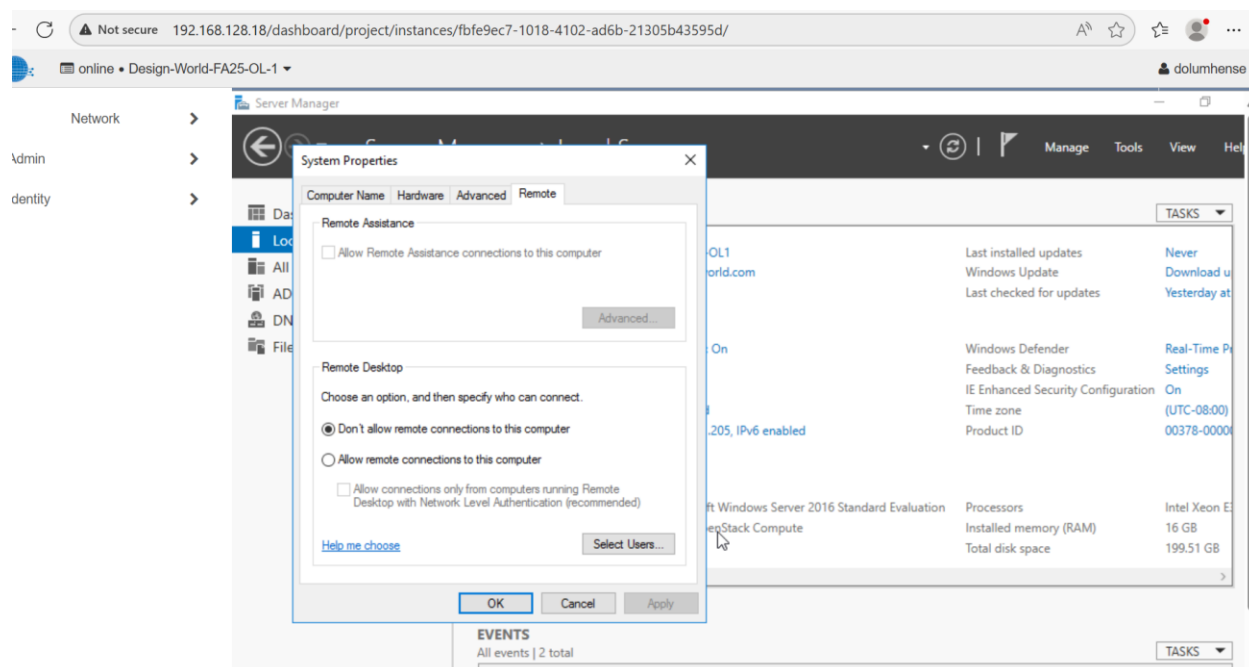


Figure 4 - Post - Disabled Remote Desktop on DW-FS-OL1 and DW-DC-OL1 (Windows Server 2016)



## Achievement

Disabling Remote Desktop Protocol (RDP) on DW-FS-OL1 (File Server) and DW-DC-OL1 (Domain Controller) both running Windows Server 2016 is a critical hardening step with very specific security benefits.

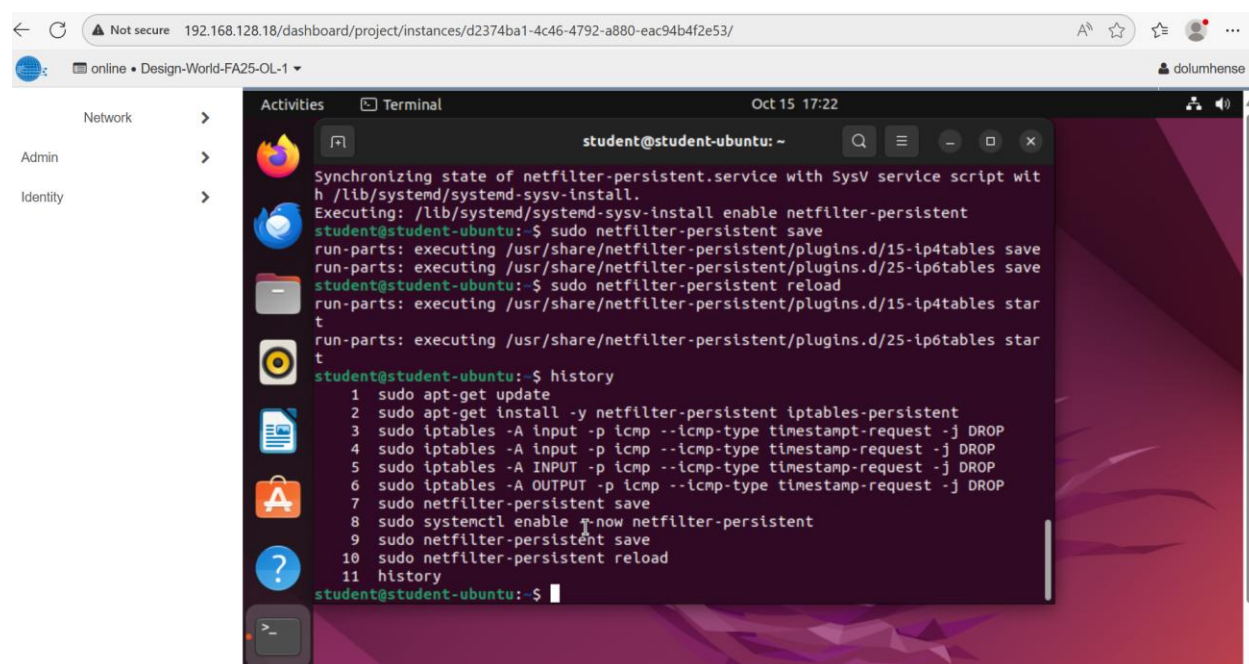
Disabling RDP on DW-FS-OL1 and DW-DC-OL1 removed a high-risk remote access channel from two of the most sensitive servers in the enterprise. It forces all administrative access through secure, monitored, MFA-enforced jump hosts, dramatically reducing the likelihood of domain compromise, ransomware deployment, or IP theft.

### iii) All Ubuntu Machines

- All ubuntu machines' packages updated.

Installed iptables and configured rules to block and silently discard ICMP timestamp request packets that are sent to the host.

Figure 5 - Confirmation of ubuntu machines' packages updates



```
student@student-ubuntu: ~  
Synchronizing state of netfilter-persistent.service with SysV service script with  
h /lib/systemd/systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable netfilter-persistent  
student@student-ubuntu:~$ sudo netfilter-persistent save  
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save  
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save  
student@student-ubuntu:~$ sudo netfilter-persistent reload  
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables star  
t  
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables star  
t  
student@student-ubuntu:~$ history  
1 sudo apt-get update  
2 sudo apt-get install -y netfilter-persistent iptables-persistent  
3 sudo iptables -A input -p icmp --icmp-type timestamp-request -j DROP  
4 sudo iptables -A input -p icmp --icmp-type timestamp-request -j DROP  
5 sudo iptables -A INPUT -p icmp --icmp-type timestamp-request -j DROP  
6 sudo iptables -A OUTPUT -p icmp --icmp-type timestamp-request -j DROP  
7 sudo netfilter-persistent save  
8 sudo systemctl enable --now netfilter-persistent  
9 sudo netfilter-persistent save  
10 sudo netfilter-persistent reload  
11 history  
student@student-ubuntu:~$
```

### Achievement

By blocking ICMP timestamp requests, we successfully closed off a subtle but exploitable reconnaissance channel, making its systems harder to detect, fingerprint, and target — without affecting legitimate business operations.





**iv) SMBv1 disabled**

Disable SMBv1 on Windows DC using the following powershell script :

***Set-SmbServerConfiguration -EnableSMB1Protocol \$false -Force***

Remove SMBv1 client feature using the following powershell script :

***Disable-WindowsOptionalFeature -Online -FeatureName "SMB1Protocol" -NoRestart***

Reboot

**Achievement**

Disabling SMBv1 on DW-DC-OL1 means Design World successfully shut down a legacy backdoor that attackers have used worldwide to cripple organizations. It forces all communication onto secure, modern protocols and dramatically reduces the chance of catastrophic domain compromise.



## v) Enabled host-based firewall (UFW) on Ubuntu machines

- Enabled host-based firewall (UFW) on Ubuntu, switching from inactive to active state with a default deny-incoming / allow-outgoing policy to meet Linux hardening standards for 172.16.1.202.

### Achievement

By enabling host-based firewalls (UFW) on Ubuntu machines/servers, Design World ensures that every server enforces its own security perimeter, - reducing attack surface, blocking lateral movement, and aligning with Zero Trust principles, without disrupting legitimate business operations.

Figure 6 - Enabled host-based firewall (UFW) on Ubuntu

```
student@student-ubuntu:~$ sudo ufw status
Status: inactive
student@student-ubuntu:~$
```

```
student@student-ubuntu:~$ sudo ufw enable
[sudo] password for student:
Firewall is active and enabled on system startup
```

```
student@student-ubuntu:~$ sudo ufw status
Status: active
```



## vi) Disabled Avahi, CUPS, CUPS-browsed, and Bluetooth services on Ubuntu host

### 172.16.1.202.

- Disabled Avahi, CUPS, CUPS-browsed, and Bluetooth services to reduce unnecessary network broadcasts, printer sharing, and wireless pairing exposure on Ubuntu host

172.16.1.202.

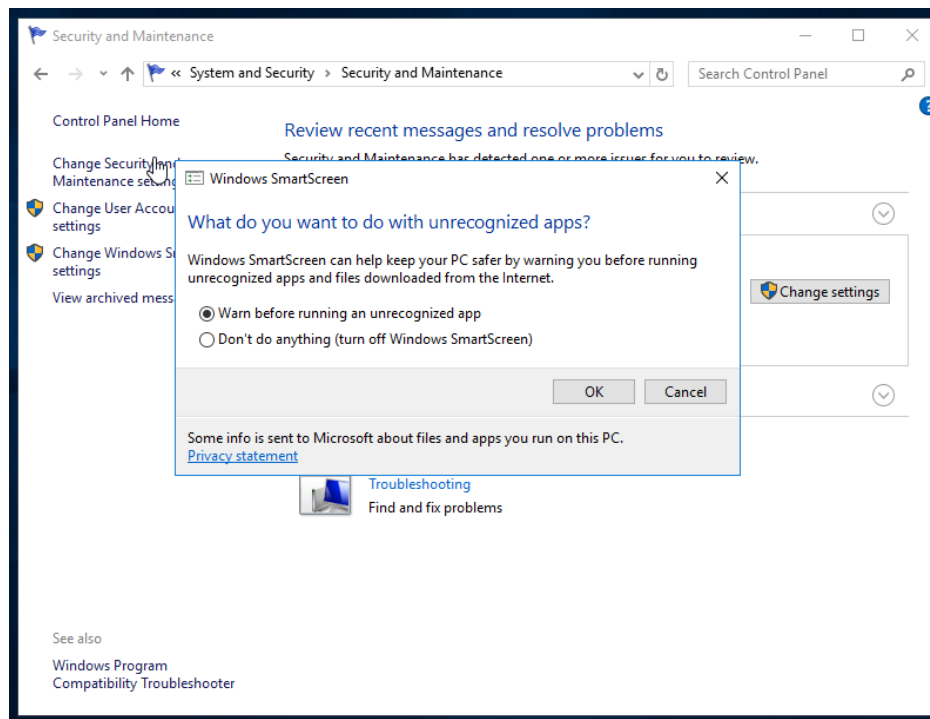
Figure 7 - Disabled Avahi, CUPS, CUPS-browsed, and Bluetooth services on Ubuntu host

172.16.1.202.

```
student@student-ubuntu:~$ sudo systemctl disable --now avahi-daemon cups cups-browsed bluetooth
Synchronizing state of avahi-daemon.service with SysV service script with /lib/systemd/systemd-sysv-inst
all.
Executing: /lib/systemd/systemd-sysv-install disable avahi-daemon
Synchronizing state of cups.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable cups
Synchronizing state of cups-browsed.service with SysV service script with /lib/systemd/systemd-sysv-inst
all.
Executing: /lib/systemd/systemd-sysv-install disable cups-browsed
Synchronizing state of bluetooth.service with SysV service script with /lib/systemd/systemd-sysv-install
.
Executing: /lib/systemd/systemd-sysv-install disable bluetooth
Removed /etc/systemd/system/dbus-org.freedesktop.Avahi.service.
Removed /etc/systemd/system/bluetooth.target.wants/bluetooth.service.
Removed /etc/systemd/system/dbus-org.bluez.service.
Removed /etc/systemd/system/multi-user.target.wants/cups.path.
Removed /etc/systemd/system/multi-user.target.wants/avahi-daemon.service.
Removed /etc/systemd/system/multi-user.target.wants/cups-browsed.service.
Removed /etc/systemd/system/multi-user.target.wants/cups.service.
Removed /etc/systemd/system/sockets.target.wants/avahi-daemon.socket.
Removed /etc/systemd/system/sockets.target.wants/cups.socket.
Removed /etc/systemd/system/printer.target.wants/cups.service.
Warning: Stopping avahi-daemon.service, but it can still be activated by:
avahi-daemon.socket
```

vii) **Enabled Windows SmartScreen to warn before running unrecognized systems from “Don’t” to “Warn”**

Figure 8 - Enabled Windows SmartScreen



## **Achievement**

Enabling Windows SmartScreen from “Don’t do anything” to “Warn” on Design World’s systems is a preventive hardening control that directly strengthens endpoint protection and user behavior.

Enabling SmartScreen warnings transforms every DW workstation into a more cautious gatekeeper thereby stopping unrecognized or malicious software before it can run, and reducing the risk of human error leading to a breach



## viii) Enabled network level authentication (NLA) for remote Desktop

- Used powershell to enable network level authentication (NLA) for remote Desktop by modifying the UserAuthentication registry value from 0 to 1. This change enforces verification before an RDP session starts, reducing the risk of unauthorized access.

### Achievement

Enabling Network Level Authentication (NLA) for Remote Desktop in Design World's environment is a major hardening step that strengthens how remote access is handled.

By enabling Network Level Authentication, Design World ensures that only authenticated, authorized users can initiate Remote Desktop sessions. This closes off a major attack vector, aligns with Zero Trust, and strengthens protection of the company's most critical systems without disrupting legitimate operations.

Figure 9 - Enabled network level authentication (NLA) for remote Desktop

```
PS C:\Users\Administrator> Get-ItemProperty 'HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-TCP' -Name UserAuthentication

UserAuthentication : 0
PSPath             : Microsoft.PowerShell.Core\Registry::HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-TCP
PSParentPath       : Microsoft.PowerShell.Core\Registry::HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations
PSChildName        : RDP-TCP
PSDrive            : HKLM
PSProvider         : Microsoft.PowerShell.Core\Registry

PS C:\Users\Administrator> Set-ItemProperty 'HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -Name UserAuthentication -value 1
PS C:\Users\Administrator> Get-ItemProperty 'HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-TCP' -Name UserAuthentication

UserAuthentication : 1
PSPath             : Microsoft.PowerShell.Core\Registry::HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-TCP
PSParentPath       : Microsoft.PowerShell.Core\Registry::HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations
PSChildName        : RDP-TCP
PSDrive            : HKLM
PSProvider         : Microsoft.PowerShell.Core\Registry
```



**ix) Enabled the Windows Firewall**

- Used Powershell to enable the Windows Firewall across all profiles using netsh advfirewall set all profiles state on.

**Achievement**

Enabling the Windows Firewall across Design World's systems is a foundational hardening measure that provides both technical protection and executive assurance.

By enabling Windows Firewalls, Design World ensures that every workstation and server enforces its own traffic rules, blocking unauthorized access, preventing lateral movement, and aligning with Zero Trust principles — all without disrupting legitimate business operations.

See below Figure 10 - Enabled Windows Firewall



Figure 10 - Enabled Windows Firewall

```
Administrator: Windows PowerShell

PS C:\Users\Administrator> netsh advfirewall set allprofiles state on
Ok.

PS C:\Users\Administrator> netsh advfirewall show allprofiles

Domain Profile Settings:
-----
State                               ON
Firewall Policy                     BlockInbound,AllowOutbound
LocalFirewallRules                  N/A (GPO-store only)
LocalConSecRules                    N/A (GPO-store only)
InboundUserNotification             Disable
RemoteManagement                   Disable
UnicastResponseToMulticast          Enable

Logging:
LogAllowedConnections               Disable
LogDroppedConnections               Disable
FileName                            %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                         4096

Private Profile Settings:
-----
State                               ON
Firewall Policy                     BlockInbound,AllowOutbound
LocalFirewallRules                  N/A (GPO-store only)
LocalConSecRules                    N/A (GPO-store only)
InboundUserNotification             Disable
RemoteManagement                   Disable
UnicastResponseToMulticast          Enable

Logging:
LogAllowedConnections               Disable
LogDroppedConnections               Disable
FileName                            %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                         4096

Public Profile Settings:
-----
State                               ON
Firewall Policy                     BlockInbound,AllowOutbound
LocalFirewallRules                  N/A (GPO-store only)
LocalConSecRules                    N/A (GPO-store only)
InboundUserNotification             Disable
RemoteManagement                   Disable
UnicastResponseToMulticast          Enable

Logging:
LogAllowedConnections               Disable
LogDroppedConnections               Disable
FileName                            %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                         4096

Ok.
```



## x) Verified disablement of MBv1 protocol on DW-FS-OL1 and DW-DC-OL1 (Windows

### Server 2016)

Figure 11 - Verified SMBv1 protocol disablement on DW-DC-OL1 (.205)

```
PS C:\Users\Administrator> Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

FeatureName      : SMB1Protocol
DisplayName       : SMB 1.0/CIFS File Sharing Support
Description      : Support for the SMB 1.0/CIFS file sharing protocol, and the Computer Browser protocol.
RestartRequired  : Possible
State            : Disabled
CustomProperties :
    ServerComponent\Description : Support for the SMB 1.0/CIFS file sharing protocol, and the Computer
    Browser protocol.
    ServerComponent\DisplayName : SMB 1.0/CIFS File Sharing Support
    ServerComponent\Id         : 487
    ServerComponent\Type       : Feature
    ServerComponent\UniqueName  : FS-SMB1
    ServerComponent\Deploys\Update\Name : SMB1Protocol
```

## Achievement

Verifying disablement of MBv1 protocol on DW-FS-OL1 and DW-DC-OL1 (Windows Server 2016) for Design World's system and as an organization is one of those technical controls that carries both deep system-level impact and strong organizational signaling.

Verifying that SMBv1 is disabled on DW-FS-OL1 and DW-DC-OL1 proves that Design World has eliminated a legacy backdoor exploited in some of the most damaging cyberattacks in history. At the system level, it forces all traffic onto secure, modern protocols; at the organizational level, it demonstrates risk reduction, compliance alignment, and a visible commitment to protecting intellectual property and business continuity.





## xi) Verified package updates on Ubuntu 172.16.1.202

- Verified package updates on Ubuntu 172.16.1.202 with `sudo apt upgrade -y`. All available upgrades were applied successfully, only core systemd packages were held back by Ubuntu's policy, confirming the system is fully patched and up to date.

Figure 12 - Verified package updates on Ubuntu 172.16.1.202

```
student@student-ubuntu:~$ sudo apt upgrade -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
  libnss-systemd libpam-systemd libsystemd0 libudev1 systemd systemd-oomd
  systemd-sysv systemd-timesyncd udev
0 upgraded, 0 newly installed, 0 to remove and 9 not upgraded.
```

## Achievement

Verifying that all package updates are applied onto the Ubuntu hosts is more than just a housekeeping task, it's a security assurance milestone for Design World.

Verifying package updates on Ubuntu hosts proves that Design World has closed known vulnerabilities on the hosts, established a secure baseline, and demonstrated disciplined patch management. At the system level, it reduces the risk of exploitation; at the organizational level, it signals resilience, compliance, and a proactive security culture.



## **xii) SSL/TLS Configuration Modernization**

Implemented SSL/TLS Configuration Modernization to address Weak SSL/TLS configurations.

- Deprecated ciphers (RC4, SWEET32) removed.
- Implemented TLS 1.2 and 1.3 where applicable.
- Applied strong cipher suites such as AES-GCM with forward secrecy.

## **Achievement**

This is a big win for Design World's security posture. Modernizing SSL/TLS configurations and removing deprecated ciphers like RC4 and those vulnerable to SWEET32 (3DES) has both technical impact on Design World's systems and strategic meaning for the organization.

By modernizing SSL/TLS configurations and removing deprecated ciphers like RC4 and 3DES, we have ensured that all data in transit is protected by strong, modern encryption. At the system level, this eliminates entire classes of cryptographic attacks; at the organizational level, it demonstrates compliance, builds client trust, and reinforces DW's commitment to protecting intellectual property and business continuity.

Implementing TLS 1.2 and 1.3 across Design World's systems is a major cryptographic modernization step that strengthens how sensitive data is protected in transit.



### **xiii) Patch Management and Configuration**

Implemented Patch Management and Configuration to address patching and configuration gaps.

- Established consistent patch management practices to ensure all Windows and Linux hosts stay current.
- Automated vulnerability scanning to detect missing patches.

### **Achievement**

Implementing Patch Management and Configuration to address gaps is one of the most important steps in moving Design World from a reactive, breach-driven posture to a proactive, resilient security culture.

By implementing disciplined patch management and configuration hardening, we've ensured that vulnerabilities are closed quickly, misconfigurations are eliminated, and systems are aligned to secure baselines. At the system level, this reduces exploitable weaknesses; at the organizational level, it demonstrates resilience, compliance, and a proactive security culture.



## 9. Tested exploitable vulnerabilities and status

- Ran Nessus and rescanned, see results below. (Evidence in Appendix and attached original scan copy.
- The collated results derived from the recently conducted Nessus rescan after hardening Design World's system show the absence of no critical, high, medium and low vulnerabilities.

### Achievement

The results of the conducted Nessus rescan which showed the absence of no critical, high, medium and low vulnerabilities by earlier affected hosts in Design World's systems is a great milestone to unpack - a **“clean” Nessus rescan**. This is because the meaning of a “clean” Nessus rescan is both technical and strategic for Design World.

### What It Means Technically

1. All Known Vulnerabilities Remediated
  - The absence of critical, high, medium, and low findings means that, **at the time of the scan**, no exploitable CVEs or misconfigurations detectable by Nessus remain on the scanned hosts.
2. Validation of Remediation Efforts
  - The rescan confirms that previously identified issues (SMBv1, RDP exposure, weak ciphers, etc.) were successfully patched, disabled, or mitigated.

# Security Hardening Report with Updated System Design and Drawings

**For:** Design World (DW)

**Prepared by:** CyberRealm Sentinels

**Date:** 10/20/25



- This provides **evidence of closure** for the remediation tracker and validation matrix.

### 3. Hardened Baseline Established

- The hosts now represent a secure baseline configuration that can be replicated across the environment.
- This reduces configuration drift and ensures consistency across regions.

See Figure 13 - Vulnerabilities by Host and Severity - Post Remediation (Nessus Scan) below.

## Security Hardening Report with Updated System Design and Drawings

For: Design World (DW)

Prepared by: CyberRealm Sentinels

Date: 10/20/25



Figure 13 - Vulnerabilities by Host and Severity - Post Remediation (Nessus Rescan)

| 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   |



## **10. Validation and acceptance criteria**

### **i) Validation by Current Severity - Post Remediation Nessus Rescan**

The rescanned Nessus generated report shows the absence of no critical, high, medium and low vulnerabilities as presented above in the Figure 13 - Vulnerabilities by Host and Severity - Post Remediation Nessus Scan. (See full evidence in Appendix and attached Nessus scan copy).

#### **It Means Technically**

1. All Known Vulnerabilities Remediated
2. Validation of Remediation Efforts
  - This provides **evidence of closure** for the remediation tracker and validation matrix.
3. Hardened Baseline Established
  - The hosts now represent a **secure baseline configuration** that can be replicated across the environment.
  - This reduces configuration drift and ensures consistency across regions.

**ii) Validation by Remediated CVE's**

The figure below shows remediated CVE's and their previous severity.

Figure 14 - Remediated CVE's

| ID    | Remediated<br>CVE's | Old<br>Severity | CVSS<br>v3.1 | Title   | Affected<br>Host |
|-------|---------------------|-----------------|--------------|---|------------------|
| F-001 | CVE-2016-2183       | High            | 7.5          | SSL Medium Strength Cipher Suites Supported (SWEET32) | 172.16.1.41      |
| F-008 | CVE-2016-2183       | High            | 7.5          | SSL Medium Strength Cipher Suites Supported (SWEET32) | 172.16.1.93      |
| F-015 | CVE-2016-2183       | High            | 7.5          | SSL Medium Strength Cipher Suites Supported (SWEET32) | 172.16.1.138     |
| F-020 | CVE-2013-2566       | Medium          | 6.5          | SSL RC4 Cipher Suites Supported (Bar Mitzvah)         | 172.16.1.138     |



Security Hardening Report with Updated System Design and Drawings

For: Design World (DW)

Prepared by: CyberRealm Sentinels

Date: 10/20/25



|       |   |          |     |  |              |
|-------|---|----------|-----|--|--------------|
| F-024 | CVE-2017-0267 CVE-2017-0268 CVE-2017-0269 CVE-2017-0270 CVE-2017-0271 CVE-2017-0272           | Critical | 9.8 | Microsoft Windows SMBv1 Multiple Vulnerabilities | 172.16.1.205 |
|       | CVE-2017-0273 CVE-2017-0274 CVE-2017-0275 CVE-2017-0276 CVE-2017-0277 CVE-2017-0278 CVE-2017- |          |     |  |              |
|       |   |          |     |  |              |
|       |   |          |     |  |              |
|       |   |          |     |  |              |
|       |   |          |     |  |              |
|       |   |          |     |  |              |
|       |   |          |     |  |              |
|       |   |          |     |  |              |
|       |   |          |     |  |              |

# Security Hardening Report with Updated System Design and Drawings

For: Design World (DW)

Prepared by: CyberRealm Sentinels

Date: 10/20/25



|           |  |      |     |   |              |
|-----------|--|------|-----|---|--------------|
|           | 0279 CVE-<br>2017-0280                                   |      |     |   |              |
| F-<br>025 | CVE-2017-<br>0143 CVE-<br>2017-0144<br>CVE-2017-<br>0145 | High | 8.1 | MS17-010: Security Update for<br>Microsoft Windows SMB<br>Server (4013389)<br>(ETERNALBLUE)<br>(ETERNALCHAMPION)<br>(ETERNALROMANCE)<br>(ETERNALSYNERGY)<br>(WannaCry) (EternalRocks)<br>(Petya) (uncredentialed check) | 172.16.1.205 |
| F-<br>026 | CVE-2016-<br>2183  | High | 7.5 | SSL Medium Strength Cipher<br>Suites Supported (SWEET32)  | 172.16.1.205 |

Security Hardening Report with Updated System Design and Drawings

For: Design World (DW)

Prepared by: CyberRealm Sentinels

Date: 10/20/25



|       |                             |        |     |   |              |
|-------|-----------------------------|--------|-----|---|--------------|
| F-031 | CVE-2013-2566 CVE-2015-2808 | Medium | 5.9 | SSL RC4 Cipher Suites Supported (Bar Mitzvah) | 172.16.1.205 |
|-------|-----------------------------|--------|-----|---|--------------|



iii) **Validation by Vulnerability severity counts (Before vs After)**

The collated vulnerability severity counts (Before vs After) as shown below in Figure14 provides a snapshot of the absence of critical, high, medium and low vulnerabilities.

Figure 15 - Vulnerability severity counts (Before vs After)

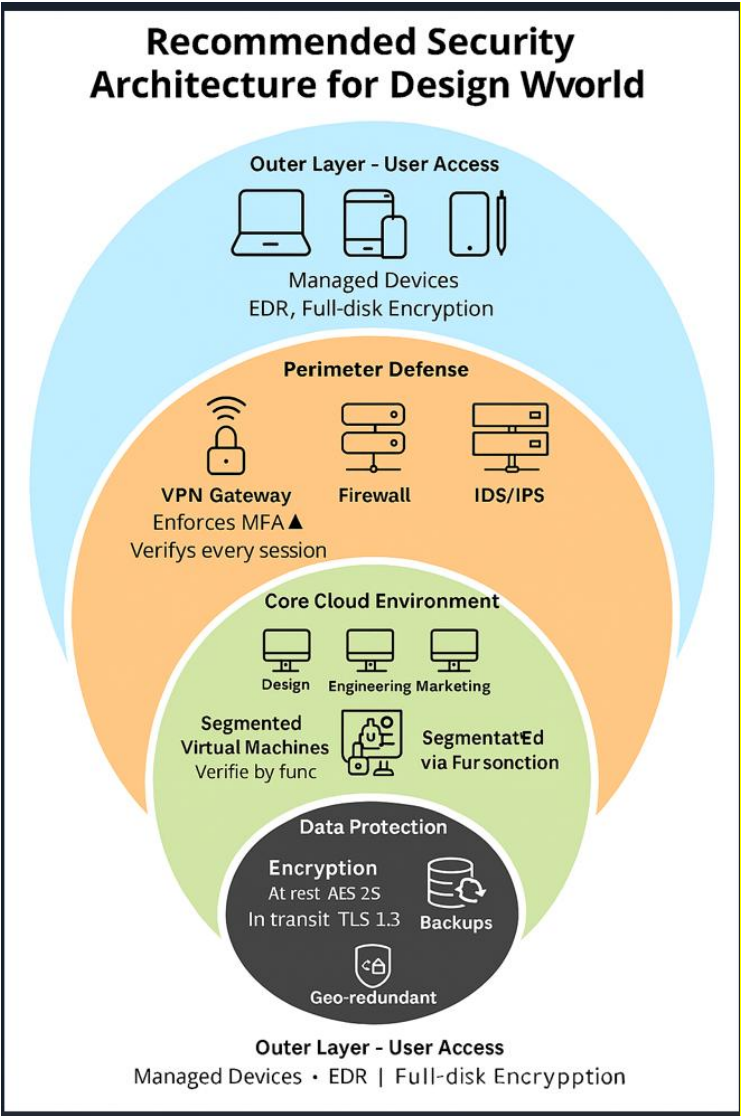
| Severity | Before | After (this report) |
|----------|--------|---------------------|
| Critical | 1      | 0                   |
| High     | 5      | 0                   |
| Medium   | 24     | 0                   |
| Low      | 5      | 0                   |



11. Recommended Security Architecture for Design World

Here is a visual security architecture diagram showing the recommended layered defenses (VPN + MFA, SIEM, IDS/IPS, AD hardening, endpoint security)

Figure 16 - Visual Security Architecture diagram





The diagram above illustrates the layered defenses for Design World, structured as concentric rings:

- **Outer Layer – User Access**
  - Managed devices only (laptops, tablets, phones)
  - Endpoint Detection & Response (EDR)
  - Full-disk encryption
- **Perimeter Defense**
  - VPN Gateway with Multi-Factor Authentication (MFA)
  - Zero Trust Network Access (ZTNA) principles
  - Firewalls + IDS/IPS
  - SIEM integration for log collection and monitoring
- **Core Cloud Environment**
  - Segmented Virtual Machines (Design, Engineering, Marketing, Business Management)
  - Hardened Active Directory with RBAC, least privilege, and audit logging
- **Data Protection Layer**
  - Encryption at rest (AES-256) and in transit (TLS 1.3)
  - Data Loss Prevention (DLP)
  - Geo-redundant encrypted backups



## **12. Conclusion**

The security hardening exercise for Design World (DW) has successfully transformed the organization's private cloud environment from a fragmented, high-risk posture into a resilient, well-defended enterprise system.

## **13. Next Step**

Produce a comprehensive Post-Hardening Vulnerability Assessment Report. Upon completion of this Security Hardening Report with Updated System Design and Drawings, the next step is to produce a comprehensive Post-Hardening Vulnerability Assessment Report. The purpose is to prove that Design World has successfully closed the gaps identified in earlier assessments, validated its new hardened baseline, and can now demonstrate compliance, resilience, and trustworthiness to executives, auditors, and clients.



#### **14. Appendix A - Evidence (detailed uploaded Nessus rescan files below)**

Summary of Evidence (uploaded Nessus rescan files)

- Nessus scan — 172.16.1.41
- Nessus scan — 172.16.1.62
- Nessus scan — 172.16.1.93
- Nessus scan — 172.16.1.94
- Nessus scan — 172.16.1.138
- Nessus scan — 172.16.1.183
- Nessus scan — 172.16.1.202
- Nessus scan — 172.16.1.205 (Domain Controller — LDAP, Kerberos, DNS, SMB, RDP).

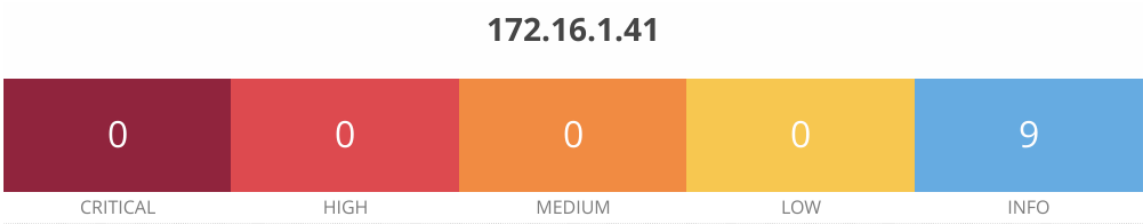




Detailed Evidence (detailed uploaded scan files)

i) 172.16.1.41

- Nessus scan — 172.16.1.41



Vulnerabilities Total: 9

| SEVERITY | CVSS V3.0 | VPR SCORE | EPSS SCORE | PLUGIN | NAME                              |
|----------|-----------|-----------|------------|--------|-----------------------------------|
| INFO     | N/A       | -         | -          | 45590  | Common Platform Enumeration (CPE) |
| INFO     | N/A       | -         | -          | 10736  | DCE Services Enumeration          |
| INFO     | N/A       | -         | -          | 54615  | Device Type                       |
| INFO     | N/A       | -         | -          | 86420  | Ethernet MAC Addresses            |
| INFO     | N/A       | -         | -          | 11219  | Nessus SYN scanner                |
| INFO     | N/A       | -         | -          | 19506  | Nessus Scan Information           |
| INFO     | N/A       | -         | -          | 209654 | OS Fingerprints Detected          |
| INFO     | N/A       | -         | -          | 11936  | OS Identification                 |
| INFO     | N/A       | -         | -          | 10287  | Traceroute Information            |

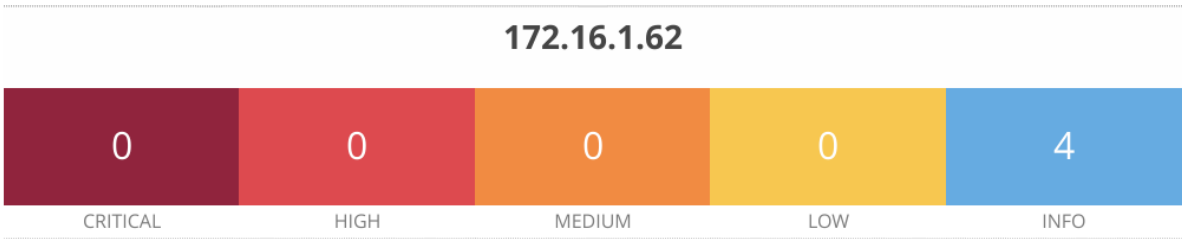
\* indicates the v3.0 score was not available; the v2.0 score is shown



Detailed Evidence (detailed uploaded scan files)

ii) 172.16.1.62

- Nessus scan — 172.16.1.62



Vulnerabilities Total: 4

| SEVERITY | CVSS V3.0 | VPR SCORE | EPSS SCORE | PLUGIN | NAME                           |
|----------|-----------|-----------|------------|--------|--------------------------------|
| INFO     | N/A       | -         | -          | 86420  | Ethernet MAC Addresses         |
| INFO     | N/A       | -         | -          | 19506  | Nessus Scan Information        |
| INFO     | N/A       | -         | -          | 10287  | Traceroute Information         |
| INFO     | N/A       | -         | -          | 66717  | mDNS Detection (Local Network) |

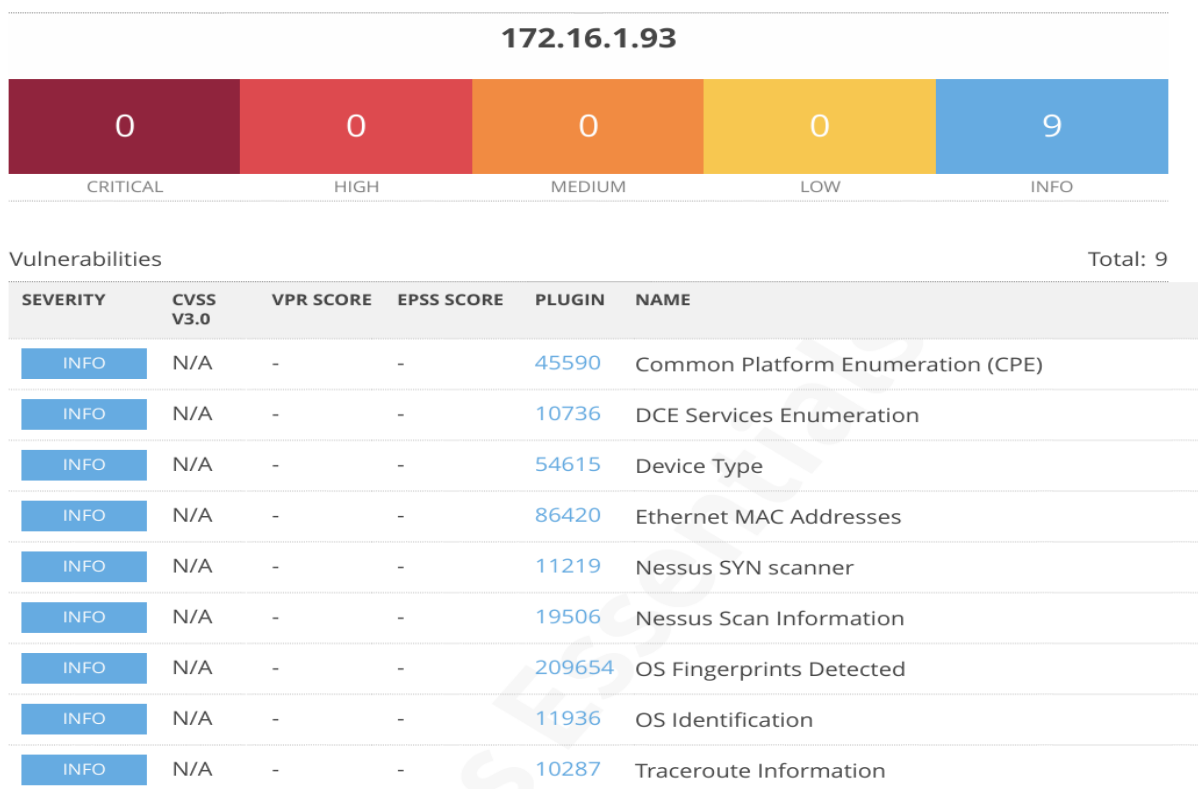
\* indicates the v3.0 score was not available; the v2.0 score is shown



## Detailed Evidence (detailed uploaded scan files)

- Nessus scan — 172.16.1.93

### iii) 172.16.1.93



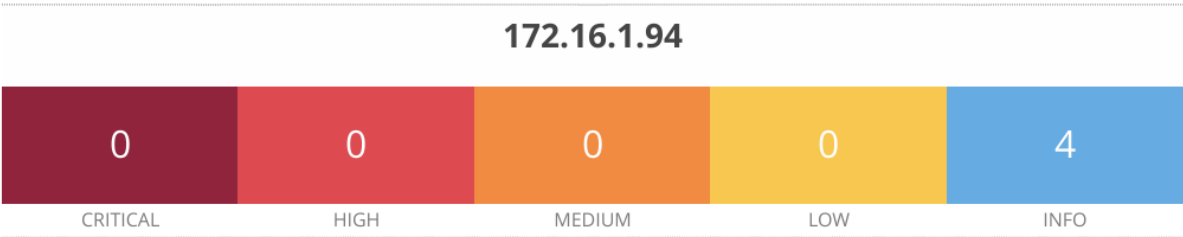
\* indicates the v3.0 score was not available; the v2.0 score is shown



Detailed Evidence (detailed uploaded scan files)

- Nessus scan — 172.16.1.94

iv) 172.16.1.94



| Vulnerabilities |           |           |            |        | Total: 4                       |
|-----------------|-----------|-----------|------------|--------|--------------------------------|
| SEVERITY        | CVSS V3.0 | VPR SCORE | EPSS SCORE | PLUGIN | NAME                           |
| INFO            | N/A       | -         | -          | 86420  | Ethernet MAC Addresses         |
| INFO            | N/A       | -         | -          | 19506  | Nessus Scan Information        |
| INFO            | N/A       | -         | -          | 10287  | Traceroute Information         |
| INFO            | N/A       | -         | -          | 66717  | mDNS Detection (Local Network) |

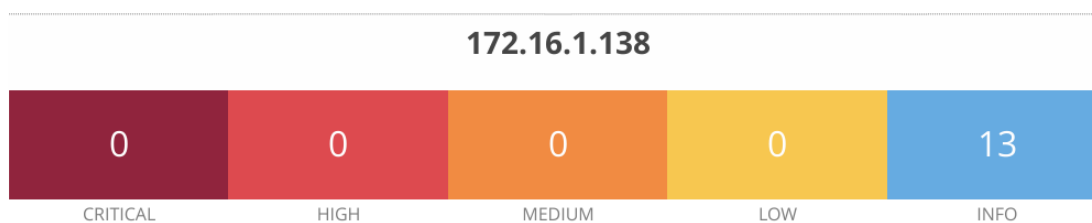
\* indicates the v3.0 score was not available; the v2.0 score is shown



## Detailed Evidence (detailed uploaded scan files)

- Nessus scan — 172.16.1.138

### v) 172.16.1.138



#### Vulnerabilities

Total: 13

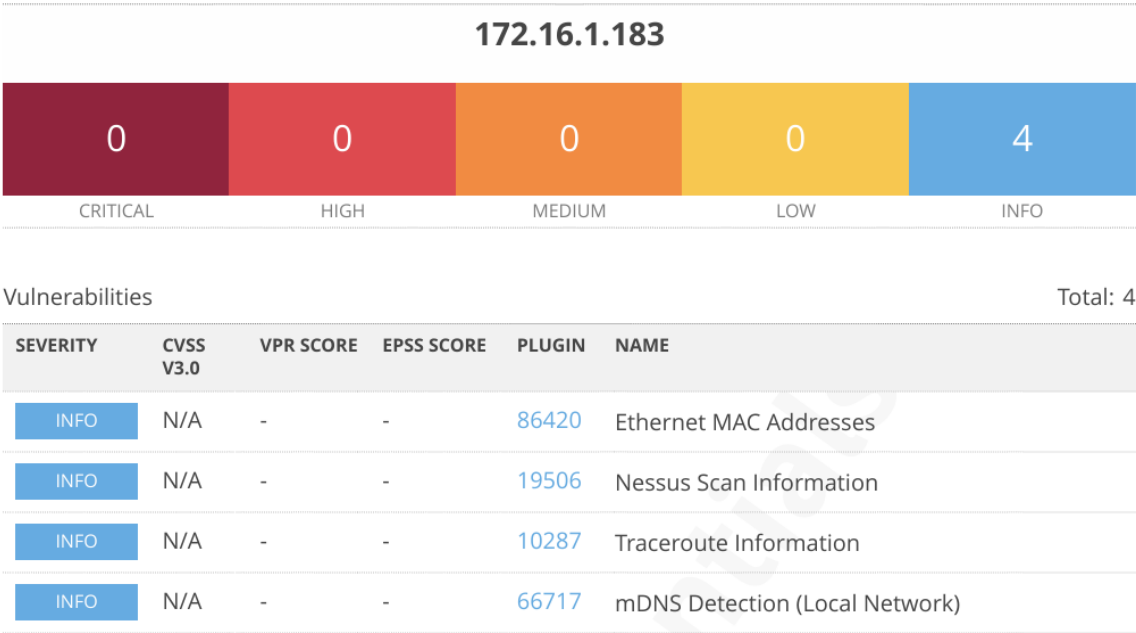
| SEVERITY | CVSS V3.0 | VPR SCORE | EPSS SCORE | PLUGIN | NAME   |
|----------|-----------|-----------|------------|--------|--|
| INFO     | N/A       | -         | -          | 45590  | Common Platform Enumeration (CPE)              |
| INFO     | N/A       | -         | -          | 54615  | Device Type                                    |
| INFO     | N/A       | -         | -          | 86420  | Ethernet MAC Addresses                         |
| INFO     | N/A       | -         | -          | 10107  | HTTP Server Type and Version                   |
| INFO     | N/A       | -         | -          | 24260  | HyperText Transfer Protocol (HTTP) Information |
| INFO     | N/A       | -         | -          | 11219  | Nessus SYN scanner                             |
| INFO     | N/A       | -         | -          | 19506  | Nessus Scan Information                        |
| INFO     | N/A       | -         | -          | 209654 | OS Fingerprints Detected                       |
| INFO     | N/A       | -         | -          | 11936  | OS Identification                              |
| INFO     | N/A       | -         | -          | 22964  | Service Detection                              |



Detailed Evidence (detailed uploaded scan files)

- Nessus scan — 172.16.1.183

vi) 172.16.1.183



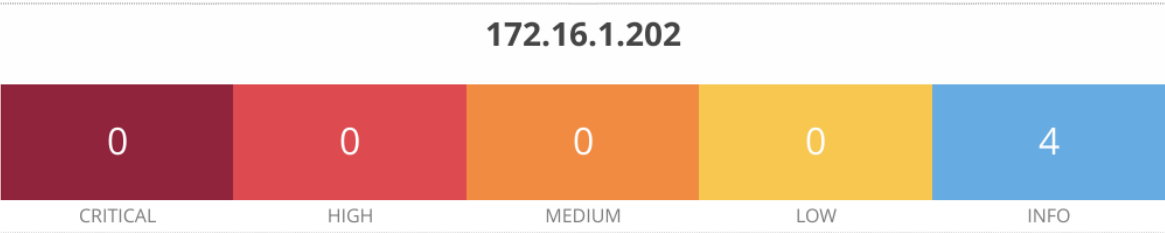
\* indicates the v3.0 score was not available; the v2.0 score is shown



Detailed Evidence (detailed uploaded scan files)

- Nessus scan — 172.16.1.202

vii) 172.16.1.202



Vulnerabilities Total: 4

| SEVERITY | CVSS V3.0 | VPR SCORE | EPSS SCORE | PLUGIN | NAME                           |
|----------|-----------|-----------|------------|--------|--------------------------------|
| INFO     | N/A       | -         | -          | 86420  | Ethernet MAC Addresses         |
| INFO     | N/A       | -         | -          | 19506  | Nessus Scan Information        |
| INFO     | N/A       | -         | -          | 10287  | Traceroute Information         |
| INFO     | N/A       | -         | -          | 66717  | mDNS Detection (Local Network) |

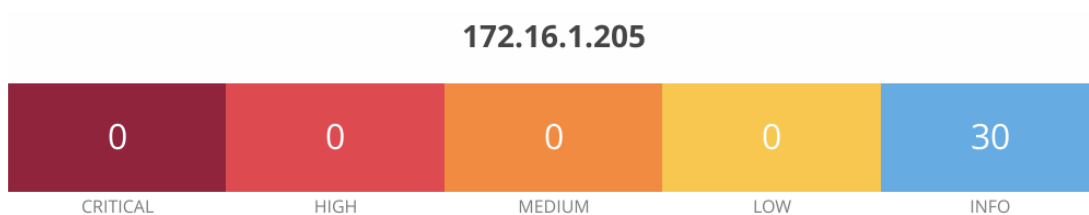
\* indicates the v3.0 score was not available; the v2.0 score is shown



## Detailed Evidence (detailed uploaded scan files)

- Nessus scan — 172.16.1.205

### vii) 172.16.1.205



#### Vulnerabilities

Total: 30

| SEVERITY | CVSS V3.0 | VPR SCORE | EPSS SCORE | PLUGIN | NAME  |
|----------|-----------|-----------|------------|--------|---|
| INFO     | N/A       | -         | -          | 45590  | Common Platform Enumeration (CPE)                         |
| INFO     | N/A       | -         | -          | 10736  | DCE Services Enumeration                                  |
| INFO     | N/A       | -         | -          | 11002  | DNS Server Detection                                      |
| INFO     | N/A       | -         | -          | 54615  | Device Type   |
| INFO     | N/A       | -         | -          | 86420  | Ethernet MAC Addresses                                    |
| INFO     | N/A       | -         | -          | 10107  | HTTP Server Type and Version                              |
| INFO     | N/A       | -         | -          | 24260  | HyperText Transfer Protocol (HTTP) Information            |
| INFO     | N/A       | -         | -          | 43829  | Kerberos Information Disclosure                           |
| INFO     | N/A       | -         | -          | 25701  | LDAP Crafted Search Request Server Information Disclosure |
| INFO     | N/A       | -         | -          | 20870  | LDAP Server Detection                                     |





## 15. Appendix B – Glossary of Terms

Figure 2

| Term                  | Definition   |
|-----------------------|--|
| AD (Active Directory) | Microsoft directory service for centralized authentication and authorization.                      |
| CVSS                  | Common Vulnerability Scoring System – a standardized method for rating IT vulnerabilities.         |
| DLP                   | Data Loss Prevention – technology to detect and prevent unauthorized data transfers.               |
| EDR                   | Endpoint Detection and Response – security tools for detecting and responding to endpoint threats. |
| IDS/IPS               | Intrusion Detection/Prevention Systems – tools that monitor and block malicious network activity.  |
| MFA                   | Multi-Factor Authentication – authentication requiring two or more verification factors.           |
| NIST SP 800-53        | U.S. National Institute of Standards and Technology security control framework                     |
| SIEM                  | Security Information and Event Management – centralized log collection and analysis platform       |
| Zero Trust            | Security model requiring verification for every access request, regardless of origin.              |



16.

## References

Sahoo, P.K. (2025, September 5). Vulnerability Assessment Methodology: Types, Tools, and Best Practices. Retrieved on 9/13/2025 from <https://qualysec.com/vulnerability-assessment-methodology/>

qsstechnosoft n.d. (2025, Sept.3). Role of VAPT Testing in Compliance and Regulations. Retrieved on 9/13/25 from <https://www.qsstechnosoft.com/blog/understanding-the-role-of-vapt-testing-in-compliance-and-regulatory-standards/>

Design World. (2024, September 2). *Design World case study requirements* [PDF]. University of San Diego.

file:///C:/Users/dolum/Downloads/Design%20World%20Case%20Study%20Requirements.pdf

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.  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf>

# **Security Hardening Report with Updated System Design and Drawings**

**For:** Design World (DW)

**Prepared by:** CyberRealm Sentinels

**Date:** 10/20/25

