CyberRealm Sentinels - Guardians of Partnered Firms

Vulnerability Assessment Report for Design World

9/22/2025

Content

1. Executive Summary

Following the successful completion of a comprehensive vulnerability assessment of Design World's assigned hosts, performed from 9/21/2025 to 9/24/2025 by the security engineering team, the assessment identified over 34 vulnerabilities across critical systems, ranging from critical to low severity. If left unaddressed, these identified high-risk issues will directly affect Design World's intellectual property to potential compromise.

Key Findings

Some key findings are classified as follows:

Critical: Microsoft Windows SMB1 Multiple Vulnerabilities on Host 172.16.1.205. The remote Windows host is affected by multiple vulnerabilities.

High: The remote Windows host, 172.16.1.205, is affected by multiple vulnerabilities.
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check).

The remote service 172.16.1.205 supports the use of medium strength SSL ciphers that are considerably easier to circumvent (medium strength encryption) - SSL Medium Strength Cipher Suites Supported (SWEET32).

Medium: SSL Certificate Cannot be trusted on host 172.16.1.41. Exposed Remote Desktop Protocol (RDP) service on Windows 10 host (172.16.1.93). While Network Level Authentication (NLA) is enabled, the service remains a common attack target.

Low: The remote Windows host, 172.16.1.62 answers to an ICMP timestamp request. It is possible to determine the exact time set on the remote host.
Ubuntu host (172.16.1.183) presented no externally accessible services. Minimal attack surface observed; risk considered low/informational.

The Vulnerability Assessment Report

This vulnerability assessment was performed on the Design World environment to identify security weaknesses across the assigned hosts. During testing, we scanned for open ports, running services, and potential exposures using industry-standard tools.

2. Assessment Scope

As defined in the Vulnerability Assessment Plan (VAP):

Figure 1 - Table of In-Scope Systems

Instance Name	IP Address	Operating System	Role / Function	Resources
DW-DC-OL1	172.16.1.205	Windows Server 2016	Domain Controller / Core Server	16 vCPUs, 200GB, 16GB RAM
DW-WIN10-2	172.16.1.41	Windows 10 Pro	User Workstation	4 vCPUs, 200GB, 16GB RAM
DW-WIN10-1	172.16.1.93	Windows 10 Pro	User Workstation	4 vCPUs, 200GB, 16GB RAM
DW-FS-OL1	172.16.1.138	Windows Server 2016	File Server (per instance list)	16 vCPUs, 200GB, 16GB RAM

Design-World-FA25-OL-1-Ubuntu-4	172.16.1.62	Ubuntu Linux	Linux Server (general-purpose)	4 vCPUs, 200GB, 16GB RAM
Design-World-FA25-OL-1-Ubuntu-3	172.16.1.94	Ubuntu Linux	Linux Server (general-purpose)	4 vCPUs, 200GB, 16GB RAM
Design-World-FA25-OL-1-Ubuntu-2	172.16.1.202	Ubuntu Linux	Linux Server (general-purpose)	4 vCPUs, 200GB, 16GB RAM
Design-World-FA25-OL-1-Ubuntu-1	172.16.1.183	Ubuntu Linux	Linux Server (general-purpose)	4 vCPUs, 200GB, 16GB RAM

3. Methodology

Following NIST SP 800‑115 and ISO/IEC 27001 best practices:

1. Asset Discovery – Nmap

   Nmap was used to identify live hosts and open ports within the assigned subnet. A ping sweep confirmed all hosts were responsive, and targeted service scans were performed.

2. Automated Vulnerability Scanning – Nessus Essentials.

   Nessus Essentials was utilized to execute automated vulnerability scans.

3. Manual Verification – Credentialed checks, config reviews, targeted exploitation:

4. Controlled Exploitation – Metasploit used to perform proof-of-concept only, no service disruption.
5. Reporting – CVSSv3 scoring, remediation recommendations.

   Findings were documented with supporting Nessus and Nmap output and screenshots. Severity was stated using CVSSv3 scoring and categorized as Critical, High, Medium and Low.

4. Findings Summary

Figure 3 - Table of Findings Summary

ID	CVE	Severity	**CVSS v3.1**	Title	Affected Host
F-001	CVE-2016-2183	High	7.5	SSL Medium Strength Cipher Suites Supported (SWEET32)	172.16.1.41
F-002	N/A	Medium	6.5	SSL Certificate Cannot Be Trusted	172.16.1.41
F-003	N/A	Medium	6.5	SSL Self-Signed Certificate	172.16.1.41
F-004	N/A	Medium	6.5	TLS Version 1.0 Protocol Detection	172.16.1.41
F-005	N/A	Medium	6.5	TLS Version 1.1 Deprecated Protocol.	172.16.1.41

F-006	N/A	Medium	4.0	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	172.16.1.41
F-007	CVE-1999-0524	Low	2.1*	ICMP Timestamp Request Remote Date Disclosure	172.16.1.62
F-008	CVE-2016-2183	High	7.5	SSL Medium Strength Cipher Suites Supported (SWEET32)	172.16.1.93
F-009	N/A	Medium	6.5	SSL Certificate Cannot Be Trusted	172.16.1.93
F-010	N/A	Medium	6.5	SSL Self-Signed Certificate	172.16.1.93
F-011	N/A	Medium	6.5	TLS Version 1.0 Protocol Detection	172.16.1.93
F-012	N/A	Medium	6.5	TLS Version 1.1 Deprecated Protocol	172.16.1.93
F-013	N/A	Medium	4.0	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	172.16.1.93

F-014	CVE-1999-0524	Low	2.1*	ICMP Timestamp Request Remote Date Disclosure	172.16.1.94
F-015	CVE-2016-2183	High	7.5	SSL Medium Strength Cipher Suites Supported (SWEET32)	172.16.138
F-016	N/A	Medium	6.5	SSL Certificate Cannot Be Trusted	172.16.1.138
F-017	N/A	Medium	6.5	SSL Self-Signed Certificate	172.16.1.138
F-018	N/A	Medium	6.5	TLS Version 1.0 Protocol Detection	173.16.1.138
F-019	N/A	Medium	6.5	TLS Version 1.1 Deprecated Protocol	173.16.1.138
F-020	CVE-2013-2566 CVE-2015-2808	Medium	6.5	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	172.16.1.138
F-021	N/A	Medium	4.0	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	172.16.1.138

F-022	CVE-1999-0524	Low	2.1*	ICMP Timestamp Request Remote Date Disclosure	172.16.1.183
F-023	CVE-1999-0524	Low	2.1*	ICMP Timestamp Request Remote Date Disclosure	172.16.1.202

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

	-0278 CVE-2017 -0279 CVE-2017 -0280				
F-025	CVE-2017 -0143 CVE-2017 -0144 CVE-2017 -0145 CVE-2017 -0146 CVE-2017 -0147 CVE-2017 -0148	High	8.1	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	172.16.1.205

F-026	CVE-2016-2183	High	7.5	SSL Medium Strength Cipher Suites Supported (SWEET32)	172.16.1.205
F-027	N/A	Medium	6.5	SSL Certificate Cannot Be Trusted	172.16.1.205
F-028	N/A	Medium	6.5	SSL Self-Signed Certificate	172.16.1.205
F-029	N/A	Medium	6.5	TLS Version 1.0 Protocol Detection	172.16.1.205
F-030	N/A	Medium	6.5	TLS Version 1.1 Deprecated Protocol	172.16.1.205
F-031	CVE-2013-2566 CVE-2015-2808	Medium	5.9	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	172.16.1.205
F-032	N/A	Medium	5.3	SSL Certificate with Wrong Hostname	172.16.1.205
F-033	N/A	Medium	4.0	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	172.1.1.205

F-034	N/A	Medium	6.8	Exposed RDP Service on Windows 10	172.16.1.93
F-035	N/A	Low	N/A	No externally accessible services	172.16.1.183

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

5. Detailed Findings & Recommendations

Figure 5.1 – Details of finding ID VULN-2025-F-001.

Finding ID	**VULN-2025-F-001**
Title	SSL Medium Strength Cipher Suites Supported (SWEET32)
Description	The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

	Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.
Risk Rating	Medium (CVSS ~7.5)
CVE	CVE-2016-2183
Affected Host	172.16.1.41
Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp) .
Recommendation	Reconfigure the affected application, if possible, to avoid use of medium strength ciphers.
Status	Open

Figure 5.2 – Details of Finding ID VULN-2025-F-002.

Finding ID	**VULN-2025-F-002**
Title	SSL Certificate Cannot Be Trusted
Description	The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below : 1) First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. 2) Second, the certificate chain may contain a certificate that is not valid at the time of the scan. 3) Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified.
Risk Rating	Medium (CVSS ~ 6.5)
CVE	N/A
Affected Host	172.16.1.41

Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Purchase or generate a proper SSL certificate for this service.
Status	Open

Figure 5.3 – Details of Finding ID VULN-2025-F-003.

Finding ID	**VULN-2025-F-003**
Title	SSL Self-Signed Certificate
Description	The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the middle attack against the remote host.
Risk Rating	Medium (CVSS ~ 6.5)

CVE	N/A
Affected Host	172.16.1.41
Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Purchase or generate a proper SSL certificate for this service.
Status	Open

Figure 5.4 – Details of Finding ID VULN-2025-F-004.

Finding ID	**VULN-2025-F-004**
Title	TLS Version 1.0 Protocol Detection

Description	The remote service encrypts traffic using an older version of TLS. The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has several cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.
Risk Rating	Medium (CVSS ~ 6.5)
CVE	N/A
Affected Host	172.16.1.41

Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.
Status	Open

Figure 5.5 – Finding ID VULN-2025-F-005 Details

Finding ID	**VULN-2025-F-005**
Title	TLS Version 1.1 Deprecated Protocol.
Description	The remote service encrypts traffic using an older version of TLS. The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

	As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.
Risk Rating	Medium (CVSS ~ 6.5)
CVE	N/A
Affected Host	172.16.1.41
Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.
Status	Open

Figure 5.6 – Details of Finding ID VULN-2025-F-006.

Finding ID	**VULN-2025-F-006**
Title	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
Description	The remote Terminal Services doesn't use Network Level Authentication only. The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established
Risk Rating	Medium (CVSS ~ 4.0)
CVE	N/A

Affected Host	172.16.1.41
Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.
Status	Open

Figure 5.7 – Details of Finding ID VULN-2025-F-007.

Finding ID	**VULN-2025-F-007**
Title	ICMP Timestamp Request Remote Date Disclosure

Description	It is possible to determine the exact time set on the remote host. The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time based authentication protocols.
Risk Rating	Low (CVSS ~ 2.1)* (* indicates that the v3.0 score was not available; the v2.0 score is shown)
CVE	CVE-1999-0524
Affected Host	172.16.1.62
Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).
Status	Open

Figure 5.8 – Details of Finding ID VULN-2025-F-008.

Finding ID	**VULN-2025-F-008**
Title	SSL Medium Strength Cipher Suites Supported (SWEET32)
Description	The remote service supports the use of medium strength SSL ciphers. The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.
Risk Rating	Medium (CVSS ~ 7.5)
CVE	CVE-2016-2183
Affected Host	172.16.1.93

Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Reconfigure the affected application if possible to avoid use of medium strength ciphers.
Status	Open

Figure 5.9 – Details of Finding ID VULN-2025-F-009.

Finding ID	**VULN-2025-F-009**
Title	SSL Certificate Cannot Be Trusted
Description	The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below : - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either

	when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority. - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates. - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the middle attacks against the remote host.
Risk Rating	Medium (CVSS ~ 6.5)

CVE	N/A
Affected Host	172.16.1.93
Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Purchase or generate a proper SSL certificate for this service.
Status	Open

Figure 5.10 – Details of Finding ID VULN-2025-F-010.

Finding ID	**VULN-2025-F-010**
Title	SSL Self-Signed Certificate.
Description	The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Risk Rating	Medium (CVSS ~ 6.5)
CVE	N/A
Affected Host	172.16.1.93
Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Purchase or generate a proper SSL certificate for this service.
Status	Open

Figure 5.11 – Details of Finding ID VULN-2025-F-011.

Finding ID	**VULN-2025-F-011**
Title	TLS Version 1.0 Protocol Detection

Description	The remote service encrypts traffic using an older version of TLS. The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.
Risk Rating	Medium (CVSS ~ 6.5)
CVE	N/A
Affected Host	172.16.1.93
Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.
Status	Open

Figure 5.12 – Details of Finding ID VULN-2025-F-012.

Finding ID	**VULN-2025-F-012**
Title	TLS Version 1.1 Deprecated Protocol
Description	The remote service encrypts traffic using an older version of TLS. The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1 As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.
Risk Rating	Medium (CVSS ~ 6.5)
CVE	N/A
Affected Host	172.16.1.93

Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.
Status	Open

Figure 5.13 – Details of Finding ID VULN-2025-F-013.

Finding ID	**VULN-2025-F-013**
Title	Terminal Services Doesn’t Use Network Level Authentication (NLA) Only.
Description	The remote Terminal Services doesn't use Network Level Authentication only. The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against

	man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.
Risk Rating	Medium (CVSS ~ 4.0)
CVE	N/A
Affected Host	172.16.1.93
Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.
Status	Open

Figure 5.14 – Details of Finding ID VULN-2025-F-014

Finding ID	**VULN-2025-F-014**
Title	ICMP Timestamp Request Remote Date Disclosure.
Description	It is possible to determine the exact time set on the remote host. The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time based authentication protocols.
Risk Rating	Low (CVSS ~2.1) * (* indicates the v3.0 score was not available; the v2.0 score is shown)
CVE	CVE-1999-0524
Affected Host	172.16.1.94
Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Status	Open

Figure 5.15 – Details of Finding ID VULN-2025-F-015.

Finding ID	**VULN-2025-F-015**
Title	SSL Medium Strength Cipher Suites Supported (SWEET32).
Description	The remote service supports the use of medium strength SSL ciphers. The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.
Risk Rating	High (CVSS ~7.5)

CVE	CVE-2016-2183
Affected Host	172.16.1.138
Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Reconfigure the affected application if possible to avoid use of medium strength ciphers.
Status	Open

Figure 5.16 – Details of Finding ID VULN-2025-F-016.

Finding ID	**VULN-2025-F-016**
Title	SSL Certificate Cannot Be Trusted.
Description	The SSL certificate for this service cannot be trusted.

	The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below : - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified.
Risk Rating	Medium (CVSS ~6.5)
CVE	N/A
Affected Host	172.16.1.138
Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Purchase or generate a proper SSL certificate for this service.
Status	Open

Figure 5.17 – Details of Finding ID VULN-2025-F-017.

Finding ID	**VULN-2025-F-017**
Title	SSL Self-Signed Certificate
Description	The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the middle attack against the remote host
Risk Rating	Medium (CVSS ~6.5)
CVE	N/A
Affected Host	172.16.1.138
Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Purchase or generate a proper SSL certificate for this service.

Status	Open

Figure 5.18 – Details of Finding ID VULN-2025-F-018.

Finding ID	**VULN-2025-F-018**
Title	TLS Version 1.0 Protocol Detection
Description	The remote service encrypts traffic using an older version of TLS.
Risk Rating	Medium (CVSS ~6.5)
CVE	N/A

Affected Host	172.16.1.138
Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	. Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.
Status	Open

Figure 5.19 – Details of Finding ID VULN-2025-F-019.

Finding ID	**VULN-2025-F-019**
Title	TLS Version 1.1 Deprecated Protocol
Description	The remote service encrypts traffic using an older version of TLS. The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that

	support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1
Risk Rating	Medium (CVSS ~6.5)
CVE	N/A
Affected Host	172.16.1.138
Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	. Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.
Status	Open

Figure 5.20 – Details of Finding ID VULN-2025-F-020.

Finding ID	**VULN-2025-F-020**
Title	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Description	The remote service supports the use of the RC4 cipher. The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness. If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.
Risk Rating	Medium (CVSS ~5.9)
CVE	N/A
Affected Host	172.16.1.138

Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recomendation	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.
Status	Open

Figure 5.21 – Details of Finding ID VULN-2025-F-021.

Finding ID	**VULN-2025-F-021**
Title	Terminal Services Doesn't Use Network Level Authentication (NLA) Only.
Description	The remote Terminal Services doesn't use Network Level Authentication only.
Risk Rating	Medium (CVSS ~4.0)

CVE	N/A
Affected Host	172.16.1.138
Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.
Status	Open

Figure 5.22 – Details of Finding ID VULN-2025-F-022

Finding ID	**VULN-2025-F-022**
Title	ICMP Timestamp Request Remote Date Disclosure.

Description	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time based authentication protocols.
Risk Rating	Medium (CVSS ~2.1*)
CVE	CVE-1999-0524
Affected Host	172.16.1.183
Evidence	Nessus Plugin Output scan result (tcp/3389/msrdp)
Recommendation	Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).
Status	Open

Finding ID	VULN-2025-F-001
Title	Exposed Remote Desktop Protocol (RDP) Service on Windows Host
Description	TCP port 3389 was open on Windows 10 host 172.16.1.93. Enumeration confirmed RDP with CredSSP and SSL/TLS enabled. Exposed RDP increases risk of brute-force or protocol-based attacks.
Risk Rating	Medium (CVSS ~6.8)
Affected Assets	Windows 10 Host – DW-WIN10-1 (172.16.1.93)

Evidence	Nmap service scan and RDP enumeration (rdp-ntlm-info, rdp-enum-encryption)
Recommendation	Restrict RDP to trusted IPs/VPN users, enforce MFA and account lockouts, patch Windows, or disable RDP if not required.
Status	Open

Finding ID	**VULN-2025-F-002**
Title	Minimal Attack Surface on Ubuntu Host
Description	Nmap scans of 172.16.1.183 showed all tested ports closed (22, 80, 443, 445, 3306, 8080). No externally accessible services were detected.
Risk Rating	Low / Informational
Affected Assets	Ubuntu Host (172.16.1.183)
Evidence	Nmap service scan (`nmap_172.16.1.183_svc.txt`)

Recommendation	Maintain system patching and firewall rules. Continue periodic scans to ensure no unnecessary services are exposed.
Status	Open

6. Risk Distribution

Critical: 1

High: 5

Medium: 24

Low: 5

7. Priority Levels

- **P1 – Critical:** Immediate action (0–30 days) – vulnerabilities that could lead to direct compromise of IP or systems.
- **P2 – High:** Short-term action (31–90 days) – significant weaknesses that increase the attack surface.
- **P3 – Medium:** Medium-term action (91–180 days) – improvements to strengthen resilience.
- **P4 – Low:** Long-term action (181+ days) – optimizations and best-practice enhancements.

8. Remediation Steps

The collective implementation of all the listed solutions for each identified vulnerability will help address and enhance the firm's defenses against advanced threats, thereby strengthening its overall security posture.

For example,

- Windows Host (172.16.1.93)**:** Restrict RDP access to trusted IPs or VPN users, enforce MFA and account lockout policies, apply regular Windows updates, and disable RDP if not required.
- Ubuntu Host (172.16.1.183)**:** Maintain patch management and firewall rules; continue periodic verification to confirm services remain closed.

9. Conclusion

The execution of the Vulnerability Assessment, and the generation of a Vulnerability Assessment Report , will enable the organization to identify several critical and high-risk security gaps, which, when properly addressed, enhance Design World's defenses against advanced threats and strengthens the firm’s overall security posture.

10. Next Steps

Produce a Penetration Test Plan. Upon completion of this Vulnerability Assessment Report, the next step is to produce a comprehensive Penetration Test Plan. The purpose of this Penetration Test Plan is to simulate realistic, controlled cyber-attack scenarios against Design World’s most

critical systems. This plan will validate the effectiveness of remediation efforts and uncover any residual or newly introduced weaknesses.

Appendix A – Evidence Files

This appendix contains a structured list of raw scan outputs and enumeration results gathered during the DesignWorld vulnerability assessment. These files serve as supporting evidence for the findings documented in the report. Each file is organized by host IP addresses and labeled by tool/output type for traceability purposes.

172.16.1.205 – DW-DC-OL1 (Domain Controller, Windows Server 2016)

- scans_nonweb/nmap_nonweb_172.16.1.205.txt

- scans_nonweb/smb_172.16.1.205.txt
- scans_nonweb/rdp_172.16.1.205.txt
- scans_nonweb/ldap_172.16.1.205.txt

172.16.1.41 – DW-WIN10-2 (Workstation)

- scans_nonweb/nmap_nonweb_172.16.1.41.txt
- share_output/rdp_enum_172.16.1.41.txt
- share_output/smb_172.16.1.41.txt
- nmap_live_172.16.1.41.txt
- share_output/final_41.txt

172.16.1.93 – DW-WIN10-1 (Workstation)

- scans_nonweb/nmap_nonweb_172.16.1.93.txt
- share_output/rdp_enum_172.16.1.93.txt
- nmap_live_172.16.1.93.txt (optional)
- share_output/smb_172.16.1.93.txt
- share_output/ldap_172.16.1.93.txt

- share_output/final_172.16.1.93.txt

172.16.1.138 – DW-FS-OL1 (File Server, Windows Server 2016)

- scans_nonweb/nmap_nonweb_172.16.1.138.txt

172.16.1.62 – Ubuntu-4 (Linux)

- scans_nonweb/nmap_nonweb_172.16.1.62.txt
- nmap_live_172.16.1.62.txt
- scans_nonweb/smb_172.16.1.62.txt
- scans_nonweb/rdp_172.16.1.62.txt
- scans_nonweb/ldap_172.16.1.62.txt

172.16.1.94 – Ubuntu-3 (Linux/Quiet VM)

- scans_nonweb/nmap_nonweb_172.16.1.94.txt
- nmap_live_172.16.1.94.txt
- share_output/rdp_enum_172.16.1.94.txt (3389 closed)
- share_output/smb_172.16.1.94.txt (445 closed)
- share_output/smbclient_172.16.1.94_anon.txt (connection refused)

- share_output/ldap_172.16.1.94.txt (389/636 closed)
- share_output/ldap_rootdse_172.16.1.94.txt (cannot contact server)
- share_output/final_172.16.1.94.txt

172.16.1.202 – Ubuntu-2 (Linux)

- scans/web_quick_172.16.1.202.txt (HTTP(S) ports closed)
- scans/nmap_full_172.16.1.202.txt

172.16.1.183 – Ubuntu-1 (Linux)

- scans/top1000_172.16.1.183.txt
- scans/allports_172.16.1.183.txt
- scans/udp_top200_172.16.1.183.txt

Appendix B – Glossary of Terms

Figure 8 **– Glossary of Terms**

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.

Appendix C – Standards & Compliance References

- NIST SP 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations.
- NIST SP 800-115 – Technical Guide to Information Security Testing and Assessment.
- ISO/IEC 27001:2022 – Information Security Management Systems (ISMS) Requirements.
- OWASP Top 10 – Most critical web application security risks.
- MITRE ATT&CK Framework – Knowledge base of adversary tactics and techniques.

Appendix D – Risk Rating Methodology

Risk ratings will be assigned using the CVSS v3.1 scoring system:

- Critical (9.0–10.0) – Immediate remediation required.
- High (7.0–8.9) – Remediate within 30 days.
- Medium (4.0–6.9) – Remediate within 90 days.
- Low (0.1–3.9) – Address during routine maintenance.

Appendix E – Rules of Engagement

1. Authorized Testing Window: September 19, 2025, 8:00 PM to September 29, 2025, 6:00 PM.

2. Permitted Activities: Vulnerability scanning, configuration review, controlled exploitation.

3. Prohibited Activities: Denial-of-service testing, social engineering (unless explicitly approved).

4. Notification Protocol: Immediate reporting of critical vulnerabilities to DW's IT Director.

5. Data Handling: No sensitive data exfiltration; proof-of-concept only.

Appendix F – Communication Plan

Figure 10

Event	Recipient(s)	Method	Framework
Kick-off Meeting	Design World Leadership, IT Team	Video Conference	1 Hour
Daily Status Updates	Design World, Chief Technology Officer (CTO) - Dr. D. Magedman	Email	Daily during testing

Critical Vulnerability Alert	Design World CEO, Mr. Jack Welch, Dr. D. Magedman - CTO	Phone + Email	Within one (1) hour of discovery.
Final Report Delivery	Design World Executive Leadership	Secure File Transfer	End of Engagement
Retest Results	Design World, Chief Technology Officer (CTO) - Dr. D. Magedman	Secure File Transfer	Post-remediation

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