Introduction

A vulnerability assessment report details the findings from a systematic evaluation of vulnerabilities within Design Worlds system, network, and applications. This identifies the weaknesses and security issues that can compromise the physical and software base environment by attackers to gain unauthorized access to steal, change or disrupt services. This shows the importance of the assessment report as a valuable tool to help with risk mitigation, resource allocation and to improve to help Design World manage future vulnerabilities continuously. FMJ^{2} ran a network base scan with the following subnets:

- 172.16.102.0/24
- 172.16.120.0/24

The number of hosts discovered (20) was more than previously mentioned and while utilizing a Nexxus Essentials license FMJ^{2} was limited to only 16 IP scans. With the project manager's discretion (Josue) making the decision to scan the selected IP addresses the remaining addresses were not included in this report. With future funding from Design World, we are looking to purchase an enterprise-level license for more advanced scans. Below you can find the grouping of the CentOS servers, Domain Controller, Kali, Ubuntu and Window Based server with the vulnerabilities found and the top five mitigations or remediations to solve the vulnerabilities.

Vulnerability Assessment Report: CentOS

CentOS – Vulnerability Summary

Host 172.16.102.58 vulnerabilities

total vulnerabilities found: 19

0	0	0	2	17
CRITICAL	HIGH	MEDIUM	LOW	INFO

Low Vulnerability (2)

- Plugin ID 153953: CentOS, SSH Weak Key Exchange Algorithms Enabled
- Plugin ID 70658: CentOS, SSH Server CBC Mode Ciphers Enabled

Info Vulnerability (2)

- INFO N/A – 10114 ICMP Timestamp Request Remote Date Disclosure
- INFO N/A – 39520 Backported Security Patch Detection (SSH)

Host 172.16.102.162 vulnerabilities

total vulnerabilities found: 19

0	0	0	2	17
CRITICAL	HIGH	MEDIUM	LOW	INFO

Low Vulnerability (2)

- Plugin ID 153953: CentOS, SSH Weak Key Exchange Algorithms Enabled
- Plugin ID 70658: CentOS, SSH Server CBC Mode Ciphers Enabled

Info Vulnerability (1)

- INFO N/A – 10114 ICMP Timestamp Request Remote Date Disclosure

- INFO N/A – 39520 Backported Security Patch Detection (SSH)

A. Host 172.16.120.79 vulnerabilities

total vulnerabilities found: 19

0	0	1	2	24
CRITICAL	HIGH	MEDIUM	LOW	INFO

Medium Vulnerability (1):

- Plugin ID 11213: CentOS, HTTP Trace / Track Methods Allowed

Info Vulnerability (1)

- INFO N/A – 10114 ICMP Timestamp Request Remote Date Disclosure

After applying the needed updates and upgrades the following vulnerabilities were found with the associated hosts.

Hosts 172.16.102.58 and 172.16.102.162 both displayed similar amounts of vulnerabilities with 2-Low & 17-Informational. The two low-severity plugins are:

- ID 153953 - SSH Weak Key Exchange Algorithms Enabled
- ID 70658: CentOS, SSH Server CBC Mode Ciphers Enabled

Plugin ID 153953 is associated with the remote SSH server that is configured to allow weak key exchange encryption. To remediate this vulnerability, FMJ^2 will disable the weak algorithms to prevent this from happening again. Plugin ID 70658 is also associated with the SSH server and uses Cipher Block chaining encryption. That may allow attackers to recover plaintext messages from the ciphertext. To remediate this vulnerability, FMJ^2 will disable the CBC mode cipher encryption and enable CTR or GCM cipher mode instead. The two informational severity plugins are:

- INFO N/A – 10114 ICMP Timestamp Request Remote Date Disclosure
- INFO N/A – 39520 Backported Security Patch Detection (SSH)

Plugin ID 10114 can allow an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated remote attacker in defeating time-based dictation protocols. The solution would be to filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). Plugin ID 39520 is designed to detect if a backported security patch has been applied to the SSH service. Backporting involves newer versions of software patches applied to older versions. Allowing vulnerabilities to get mitigated without upgrading to the latest versions which might cause more issues of compatibility.

Host 172.16.120.79 displayed 1-Medium, 2-Low, and 24-Informational vulnerabilities. The medium severity plugin is:

- ID 11213 HTTP Trace / Track Methods Allowed

The HTTP Trace method is used for diagnosis purposes, allowing clients to retrieve entire request received from the server. The HTTP Track method can be misused by attackers for crosssite tracing attacks or other exploits. To mitigate this vulnerability disabling Trace and Track methods can help prevent certain types of attacks and improve the overall security posture.

Part 2: Fatima

Vulnerability Assessment Report: Domain Controller and file server & Kali

Domain Controller and File Server (DC/FC) – Vulnerability Summary

Domain Controller: A domain controller (DC) is a server that plays a central role in Windows-based networks using the Active Directory (AD) service. Its primary functions include user authentication, authorization, and management of network resources. The domain controller stores user account information, manages security policies, and handles user logins and access control. It also replicates information across multiple domain controllers for fault tolerance and scalability. Domain controllers are essential for managing large-scale networks and providing a centralized administration platform.

File Server: A file server is a computer or storage device that is dedicated to storing, organizing, and sharing files over a network. It acts as a central repository where users can store and access their files. File servers provide features such as file sharing, access control, and file permissions to ensure data security and collaboration. They allow multiple users to access files simultaneously and provide a consistent file system structure across the network. File servers can be implemented using various operating systems, including Windows Server, Linux-based systems, and Network-Attached Storage (NAS) devices.

A. Host 172.16.102.67 vulnerabilities

total vulnerabilities found: 263

42	68	17	1	135
CRITICAL	HIGH	MEDIUM	LOW	INFO

Critical Vulnerability (42)

- Plugin ID 129719: KB4519998: Windows 10 Version 1607 and Windows Server 2016 October 2019 Security Update
- Plugin ID 130906: KB4525236: Windows 10 Version 1607 and Windows Server 2016 October 2019 Security Update

- Plugin ID 149390: KB5003197: Windows 10 Version 1607 /Windows Server 2016 October 2019 Security Update (May 2021)

High Vulnerability (68)

- INFO N/A – 108967: KB4093119: Windows 10 Version 1607 /Windows Server 2016 April 2018 Security Update
- INFO N/A – 109606: KB4103723: Windows 10 Version 1607 /Windows Server 2016 May 2018 Security Update

B. Host 172.16.102.118 vulnerabilities

total vulnerabilities found: 252

41	65	18	1	127
CRITICAL	HIGH	MEDIUM	LOW	INFO

Critical Vulnerability (41)

- Plugin ID 129719: KB4519998: Windows 10 Version 1607 and Windows Server 2016 October 2019 Security Update
- Plugin ID 130906: KB4525236: Windows 10 Version 1607 and Windows Server 2016 October 2019 Security Update
- Plugin ID 136505: KB4556813: Windows 10 Version 1607 and Windows Server 2016 May 2020 Security Update

High Vulnerability (66)

- INFO N/A – 108967: KB4093119: Windows 10 Version 1607 and Windows Server 2016 April 2018 Security Update
- INFO N/A – 109606: KB4103723: Windows 10 Version 1607 /Windows Server 2016 May 2018 Security Update

The top five domain controllers and file servers in the network have been identified as potential security risks due to outdated software and lack of patching. It is crucial to address these issues promptly to ensure the security and integrity of the network. By implementing regular patching and updates on these servers, we can mitigate potential vulnerabilities and enhance overall system security. Updating the domain controllers and file servers will not only address the existing security risks but also improve their performance and reliability. It is recommended to prioritize these updates and establish a proactive approach to ensure the network's resilience against potential threats.

Vulnerability Assessment Report: Kali

Kali Linux: Kali Linux is a Debian-based Linux distribution that focuses on penetration testing, digital forensics, and security auditing. It is widely used by security professionals and researchers for various cybersecurity tasks. Kali Linux comes with a vast collection of pre-installed tools and utilities specifically designed for testing and assessing the security of computer systems and networks. These tools cover areas such as network scanning, vulnerability assessment, password cracking, wireless security, and web application testing. Kali Linux provides a comprehensive platform for ethical hacking, security assessments, and educational purposes.

C. Host 172.16.102.127 vulnerabilities

total vulnerabilities found: 48

0	0	1	0	47
CRITICAL	HIGH	MEDIUM	LOW	INFO

Medium Vulnerability (1)

- Plugin ID 51192: SSL Certificate Cannot be trusted

Info Vulnerability (47)

- INFO N/A – 141394 Apache HTTP Server Installed (Linux)
- INFO N/A – 142640 Apache HTTP Sever Site Enumation

D. Host 172.16.102.209 vulnerabilities

total vulnerabilities found: 3

0	0	0	0	3
CRITICAL	HIGH	MEDIUM	LOW	INFO

Info Vulnerability (3)

- INFO N/A – 10114 ICMP Timestamp Request Remote Date Disclosure
- INFO N/A – 86420 Ethernet MAC Addresses
- INFO N/A – 19506 Nessus Scan Information

Kali is an essential tool in our network security arsenal, serving as a reliable Nessus scanner. However, due to licensing restrictions with Nessus Essentials, we need to optimize its usage by limiting its scope to specific Kali boxes. This includes grouping the computers that were updated prior to the installation of Nessus. By doing so, we can effectively manage and prioritize the findings, ensuring that we maximize the utility of our limited license. This approach allows us to focus our scanning efforts on the most critical areas of our network and optimize the overall security assessment process.

PART 3:

Vulnerability Assessment Report: Ubuntu & Windows

Ubuntu – Vulnerability Summary

A. Host 172.16.102.103 vulnerabilities

total vulnerabilities found: 40

0	0	0	0	40
Critical	High	Medium	Low	Informational

Informational vulnerabilities (42):

- INFO N/A – 10114 ICMP Timestamp Request Remote Data Disclosure
- INFO N/A – 34098 BIOS Info (SSH)

B. Host 172.16.102.214 vulnerabilities

total vulnerabilities found: 43

0	1	0	0	42
Critical	High	Medium	Low	Informational

High Vulnerabilities (1):

- Plugin ID175883: Ubuntu 20.04 LTS / 22.04 LTS: Linux kernel vulnerabilities (USN-6080-1). CVSSv3 Score: 7.8. Vulnerability Priority Rating (VPR) 7.4.

Summary

The vulnerability assessment report generated by Nessus on May 25th, 2023, reveals important insights regarding Design World's security posture of the scan system running Ubuntu. The report identifies a total of 83 vulnerabilities across two hosts, with 40 vulnerabilities found on host 172.16.102.103 and 43 vulnerabilities on host 172.16.102.214.

Host 172.16.102.103 exhibits 40 vulnerabilities, which consists entirely of informational findings. These findings cover a range of areas including network enumeration, software and service detection, SSH configuration, and system information disclosure. While no critical or high severity vulnerabilities were identified, it is important to address these informational issues to ensure the system's security and protect against potential exploitation. 10114 ICMP Timestamp Request Remote Data Disclosure, for example, can allow an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated remote attacker in defeating time-based on dictation protocols. The solution would be to filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

On the other hand, host 172.16.102.214 presents 43 vulnerabilities, including one high severity vulnerability related to Linux kernel vulnerabilities (USN-6080-1). In short, it was discovered that some AMD x86-64 processors with SMT enabled could speculatively execute instructions using the return address from a sibling thread. A local attacker, for example, could possibly use this to expose sensitive information. The problem can be corrected by updating the system to the following package version: Ubuntu 22.04. The remaining vulnerabilities are classified as informational, covering various aspects such as ICMP disclosure, device identification, network configuration, SSH related issues, patch assessment, and software enumeration. It is essential to prioritize a high severity vulnerability and promptly apply the necessary security patches to mitigate the associated risk.

Windows – Vulnerability Summary

C. Host 172.16.102.50 vulnerabilities

total vulnerabilities found: 79

0	2	7	0	70
Critical	High	Medium	Low	Informational

High Vulnerabilities (2):

- Plugin ID35291: SSL Certificates Signed Using Weak Hashing Algorithm. CVSSv3 Score: 7.5. Vulnerability Priority Rating (VPR)L 5.1

D. Host 172.16.102.55 vulnerabilities

total vulnerabilities found: 79

0	2	7	0	70
Critical	High	Medium	Low	Informational

High Vulnerabilities (2):

- Plugin ID35291: SSL Certificates Signed Using Weak Hashing Algorithm. CVSSv3 Score: 7.5. Vulnerability Priority Rating (VPR)L 5.1

E. Host 172.16.102.129 vulnerabilities

total vulnerabilities found: 79

0	2	7	0	70
Critical	High	Medium	Low	Informational

High Vulnerabilities (2):

- Plugin ID35291: SSL Certificates Signed Using Weak Hashing Algorithm. CVSSv3 Score: 7.5. Vulnerability Priority Rating (VPR)L 5.1

F. Host 172.16.102.157 vulnerabilities

total vulnerabilities found: 79

0	2	7	0	70
Critical	High	Medium	Low	Informational

High Vulnerabilities (2):

- Plugin ID35291: SSL Certificates Signed Using Weak Hashing Algorithm. CVSSv3 Score: 7.5. Vulnerability Priority Rating (VPR)L 5.1

G. Summary

The vulnerability assessment report generated by Nessus on May 25th, 2023, provides an overview of the Design World (DW) vulnerabilities found on three Windows PC hosts: 172. 16.102.50, 172.16.102.55, and 172.16.102.129. The report indicates that each host has a total of 79 vulnerabilities, categorized into critical, high, medium, low, and information security levels. Some of the critical and high severity vulnerabilities discovered include weak hashing algorithm usage and SSL certificates and support for medium- strength cipher suites.

For the host with IP address 172.16.102.50, FMJ^2 was able to discover several vulnerabilities, including weak SSL certificate signing, medium-strength cipher suite support, and issues related to SSL certificates, TLS protocols, and SMB signing. Similarly, the host with IP address 172.16.102.55 exhibits similar vulnerabilities, along with additional information disclosure issues and enumeration of users and devices. The host with IP address 172.16.102.129 also demonstrates similar vulnerabilities. The plugin ID35291: SSL Certificates Signed Using Weak Hashing Algorithm, for example, is an SSL certificate that has been signed using the weak hash algorithm. These signature algorithms are known to be vulnerable to collision attacks. The attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service. The solution would be to contact the Certificate Authority to have the SSL certificate we issued.

The vulnerability assessment report from Nessus reveals that the Windows PCs with IP addresses 172.16.102.50, 172.16.102.55, and 172.16.102.129 are susceptible to various security risks. These risks primarily involve weaknesses and SSL certificates, TLS protocols, and SMB signing, potentially exposing the systems to unauthorized access and information disclosure. It is crucial for DW to address these vulnerabilities promptly to mitigate the risk of exploitation and protect the confidentiality and integrity of their systems.

Conclusion & Next Steps

In conclusion, based on the vulnerabilities we found using the Nessus scanner, which is a version compliance scanner, we identified that the environment needs to implement some form of a patching schedule. We identified multiple hosts running operating systems far past the end of life, which opens up Design World's network to attacks. Our next step now is to scan the environment and look for configurations that can be tweaked and helped brought to compliance to help improve a computer's SCAP compliance percentage with the respected STIG.