THE RED USERS TASK 1

NETWORK VULNERABILITY ASSESSMENTS

VENKATESH VOOTA

20TH AUG 2024

Table of Contents

INTRODUCTION TO PROJECT:

The project titled “Network Vulnerability Assessment” was created with the aim of finding out what kind of vulnerabilities the company faces, as a way to not only resolve them but act as a proactive means towards avoiding future recurrences of vulnerabilities.

As the security team, it is imperative to protect the company’s systems from unauthorized personnel however with the continuous innovation of technology, staying on top of new software’s and mitigation measures to safeguard our systems is imperative and hereby acts as the motivation and rationale behind the project.

A company system or object is considered to be vulnerable when it has a weakness in its system that results in it being susceptible to attacks such as denial of service (DoS) or incidences of unauthorized access by third parties. If not attended to immediately through active defence mechanisms and preventative methods, these vulnerabilities can pave the way for cybercriminals to exploit them and result in the company system being jeopardized and the Confidentiality, Integrity and Availability (CIA triad) not being maintained. Given that ensuring systems maintain the CIA triad, vulnerability assessments are necessary.

In addition, A Company should maintain its operational integrity by complying to Cybersecurity regulations and industry compliance standards. The systems, software's and methodology adopted must be in compliance with the NIST, PCI and GDPR. As a result, scanning for vulnerabilities and areas in need of patching is necessary to be in accordance with the standards we are required to implement.

The following project aims to discover, protect and prevent future and current vulnerabilities by first discovering them using the company IP address and then identifying methods to address them and safeguard them for future purposes. Through a use of well trusted Vulnerability Scanner: Nessus and the use of Nmap, the project has adapted various sources to ensure that all vulnerabilities have been discovered. By doing so, A Company is able to maintain sensitive data, ensure only authorized personnel have access to data they require, ensure that company is complying with industry standards and maintaining integrity throughout the organization.

NETWORK VULNERABILITY TESTING:

Vulnerability testing systematically evaluates, reviews and analyses an organizations network infrastructure by finding vulnerabilities and loopholes that may jeopardize the company's security or be a method used for cyberattacks. The strength of a company's network security is determined by vulnerability testing and hereby will determine the ability of a company to maintain business continuity, protection of sensitive data, compliance and network privacy. Without

network vulnerability testing, it is impossible for a company to manage its vulnerabilities, due to the fact that it cannot begin its management process without identifying what areas require to be managed more strategically.

ASSESSMENT METHODOLODY

The project was conducted through the use of one Vulnerability scanner, and manually through the command Nmap on Kali Linux. The rationale behind using various sources and methods was to ensure a comprehensive and wide range of vulnerabilities to be detected. It was also to ensure a lack of overreliance on one source, but to implement various sources to increase accuracy in results and findings.

TOOLS:

The primary goal of Network Reconnaissance was performed using the following tools:

1. **Nessus**: Nessus is a vulnerability scanner powered by Tenable that seeks to help identify potential vulnerabilities within a system, out of compliance settings and misconfigurations that may be used by exploits for malicious purposes.
2. **Nmap**: Nmap known as “Network Mapper” is a tool that can be used on Linux as an open-source tool for Network discovery, security auditing, discovering hosts and operating systems. Nmap allows network admins to

find which devices are running on their network, discover open ports and services, and detect vulnerabilities

The tools were used for overall network reconnaissance and vulnerability scanning. Nmap was used to understand the network architecture of the company as well as understanding attack surfaces on the network including open ports and vulnerabilities. Nessus was used for vulnerabilities within the company network such as software's that are not in compliance with industry standards, potential attacks and CVE vulnerabilities according to NIST.

COMPLIANCE AND REGULATORY STANDARDS:

The assessment and project adhered to specific industry compliance standards to ensure operational integrity of the company.

1. **ISO 27000:** The ISO 27000 series is a number of best practices to help organizations improve their information security. This standard is implemented when dealing with data breaches and serves to act as a guideline in defences against these breaches for effective security.
2. **NIST CSF 8001-171:** Under this compliance, it is imperative to identify and address vulnerabilities. According to the NIST guideline, it helps with vulnerability management, as well as the security and privacy controls for organizations. It serves as a framework in the testing period.

VULNERABILITY CLASSIFICATIONS

The results that were outputted by the vulnerability scanner: Nessus were categorized according to the National Vulnerability Database Common Vulnerability Scoring system (CVSS) through five score metrics: Critical, High, Medium, Low or Informational.

1. **Critical:** These are vulnerabilities with a CVSS score of 9.0 to 10.0, that indicate they can be easily exploited by an attacker and system can be compromised.
2. **High:** Vulnerabilities with a CVSS score of 7.0 to 8.9, that indicate local users can gain privileges that can allow unauthenticated remote users to view resources or cause a denial of service.
3. **Medium:** Vulnerabilities with a CVSS score of 4.0 to 6.9, that indicate flaws that may be difficult for third parties to exploit but are cause for concern as they can still lead to compromise.
4. **Low:** Vulnerabilities with CVSS score of 0.1 to 3.9, that indicate vulnerabilities that if exploited may cause either no adverse effect or minimal adverse consequences.

ASSESSMENT FINDINGS

Through the use of two sources, Nessus identified a total of sixteen Vulnerabilities with one being" High" and three scored a CVSS of "Medium".

On the other hand, vulnerability scanning on Nmap revealed two vulnerabilities that were both categorized as “Medium”.

Below are the vulnerabilities found that are non-informational and found from the various sources. Evidence of the collated vulnerabilities can be referenced to at the end of the document.

1. **CVE-2016-2183**

   Name: SSL Medium Strength Cipher Suites Supported (SWEET32)

   Severity: High

   CVSS Score: 7.5

   Detail: The Sweet32 attack is a vulnerability that can occur through the use of some SSL Cyphers that are weak in design and offer less projection against attacks. The attack makes use of these older versions of the SSL Cyphers used in common protocols such as TLS and OpenVPN, in order for remote users to obtain plaintext data.

2. **CWE 327**

   Name: TLS Version 1.0 Protocol Detection

   Severity: Medium

   CVSS Score: 6.5

   Detail: The current system accepts the use of the TLS 1.0. This version relies on the SHA-1 hash of messages exchanged which is not secure. This

vulnerability allows an attacker to execute a downgrade attack on the handshake, compromising security far more than contemporary standards deem acceptable.

3. **CVE-2019-20372**

   Name: nginx < 1.17.7 Information Disclosure

   Severity: Medium

   CVSS Score: 5.3

   Detail: These files contain crucial server settings, including listening ports and server names. The current nginx within the system of 1.7.7 allows HTTP request smuggling which allows an attacker to read unauthorized web pages, hereby compromising the security of the system.

4. **Plugin #51192**

   Name: SSL Certificate Cannot be trusted

   Severity: Medium

   CVSS Score: 6.5

   Detail: This vulnerability occurs when the certificate is signed by an unknown authority hereby meaning it is impossible to verify its integrity. The current system is hereby using an SSL certificate that cannot be trusted. This is a vulnerability because without a trusted SSL certificate, it can lead to man in the middle exploits given its difficult to authenticate and verify the web server with the use of an untrusted certificate.

5. **Cross domain and client access policies**
   Severity: Likely vulnerable (Medium)

   CVSS Score: 6.5

   Detail: The vulnerability found within the system is due to overly permissive configurations that can pave the way for web clients and third parties to commit Cross-Site Forgery attacks and unauthorized access by third parties to sensitive data. This hereby means that the current system can be exploited and may result in the confidentiality of the system being compromised.

6. **CVE-2005-3299**

   Name: phpMyAdmin 2.6.4

   Severity: Medium

   CVSS Score: 5.0

   Detail: The current system has a PHP file inclusion vulnerability which is a web vulnerability and security flaw that allows unauthorized users to access files, provide download functionality and look for information. This vulnerability allowing remote attacks access compromises the CIA of the organizations system.

MITIGATION STRATEGIES

1. **CVE-2016-2183**

   - Reconfigure the affected application in order to ensure other parts of the system are not compromised.

- Disable and deprecate the current cipher suites in the TLS or SSL configuration.
- Disable all 3DES Ciphers
- Use of stronger encryption algorithms such as AES for stronger and trusted protection from remote user attacks.

2. **CWE 327**
    - Remove all TLS 1.0 protocol dependencies within the software.
    - Update system protocols use to TLS 1.2 and TLS 1.3
3. **CVE-2019-20372**
    - Upgrade to nginx version 1.17.7 or later versions
4. **Plugin #51192**
    - Renew SSL certificate to check whether it will update to a trusted version.
    - Purchase new SSL certificate
5. **Cross domain and client access policies**
    - Review permissions set to various web clients
    - Provide permissions using the Principle of Least privilege to web clients in order to maintain confidentiality and eliminate risk of Cross- Site forgery attacks.
    - Implement Token Synchronization, that is effective in mitigating CSRF attacks because it ensures that requests can only be made from

a valid user session. This means that even if an attacker can generate a request that looks like it comes from the user, they will not have the correct token and the request will be rejected.

6. CVE-2005-3299

- Implement Whitelisting. This is a list of trusted email addresses, IP addresses, domain names or applications or even executable files, while denying all others. By having this and only allowing trusted sources, it eliminates the risk of third parties accessing files they are not authorized to access.
- Use of databases rather than servers. Instead of saving files or information that can be compromised and have sensitive information on a web server, saving them on a database is more secure. This allows for CIA to be maintained.
- Restrict execution permissions for upload directories as well as upload file sizes.
- Run dynamic application security tests to determine if your code is vulnerable to file inclusion exploits.
- Sanitize user-supplied inputs, including GET/POST and URL parameters, cookie values, and HTTP header values. Apply validation on the server side, not on the client side.

By implementing these mitigation and remediation methods, it is possible to maintain security within the organizations system. Furthermore, by identifying the various risks the organization is vulnerable to, it has allowed us to stay ahead by making the necessary patches to our system and areas that need to be reconfigured entirely.

CONCLUSION

The project conducted by the security team at CDF was an overall success as it allowed us to identify, evaluate and protect our systems from vulnerabilities we are susceptible to as an organization. Through the use of Nessus and Nmap, six main vulnerabilities were found to exist with one being categorized as “High” while the rest maintained an overall scoring of “Medium”.

SUMMARY OF FINDINGS:

1. ***Vulnerabilities identified with a CVSS High score:*** SSL Medium Strength Cipher Suites Supported (SWEET32).
2. ***Vulnerabilities identified with a CVSS Medium score:*** TLS 1.0 version, nginx information disclosure, SSL certificate not trusted, PHP file inclusion and Cross Site forgery attacks.

KEY RECOMMENDATIONS:

The information below is a summary of the found mitigation and preventative methods that will be implemented to addressing each of the six vulnerabilities found within the systems;

1. ***Patching and Updates of system***: This includes updating of untrusted SSL certificates and update to newer versions of protocols such as the TLS 1.2 in order to ensure that system has up to date security measures and does not pave way for man in the middle potential attacks that are found within older versions of software.
2. ***Implementation of safer security measures***: This includes implementing safer habits that are more secure to the system such as use of Whitelisting that ensures only trusted and authorized sources have access rights. Furthermore, this includes reviewing of current permissions set to web servers and reconfiguring them to increase security within our systems. Finally, use of databases rather than web servers for data storage to avoid information being compromised.
3. ***Network protection and safeguarding***: This includes proactive safeguarding measures to ensure CIA of the organization systems including implementation of stronger firewalls as well as permissions to web clients being provided using the Principle of Least Privilege agenda.
4. ***Regular monitoring***: This includes consistent vulnerability assessments to ensure that not only is system equipped to handle newer cyberattack methods but to safeguard from current vulnerabilities and current exploits. Furthermore, this also includes regular monitoring through logs in order for faster detection of potential attacks or unusual activity for a more proactive approach.

The security team has made a commitment to ensuring the safety of the organizations systems, one of the ways being Vulnerability Management. Through the recommendations highlighted above, there is a commitment to security of the company and protection of our Confidentiality, Integrity and Availability from unauthorized third parties.

REFERENCES

REFERENCE 1: SWEET32 ATTACK

https://www.cisco.com/c/en/us/support/docs/cloud-systems management/cloudcenter/212151-Nmap-Shows-that-CCM-is-Susceptible-to-SW.html

REFERENCE 2: TLS 1.0 VERSION

https://www.tenable.com/plugins/nessus/1572

REFERENCE 3: nginx < 1.17.7 Information Disclosure

https://www.tenable.com/plugins/nessus/134220

REFERENCE 4: SSL Certificate Cannot be trusted

https://www.tenable.com/plugins/nessus/51192