Network Security June 2022 B

Unit 6

Assignment on Vulnerability Audit and Assessment

- Results and Executive Summary

Table of Contents

Executive summary:

The main intention of carry out the vulnerability scan is to the vulnerabilities that are present in https://tigertek.org.uk and assessment of the vulnerability based on the severity was done. The analysis of the recommendation for the elimination of the risks will be done and resolving of those issues based upon the risk severity will be made. The testing was done, and analysis of the threats were done and it is found that various threats such as website fingerprinting, common configuration issues and some of the cookie setting issues were levelled up.

Scan results:

The scan results were provided in the scan summary report attached and it provides a brief summary of risks and their impact level. The solution to defeating those risks is also mentioned on the basis of the impact level (Basit, 2011).

Methodology used:

The scanning activity was accomplished by means of the pen testing tools and discovery of the vulnerability in the host can be identified. While carry out the performing the risk assessment, the prediction of the system crash or existence of the factors that are responsible for system performance degradation will be made. The vulnerability scanning can be carried out in two phases such as: (Maham, 2019)

- Network discovery
- Vulnerability assessment

The network discovery phase was carried out for the discovery of the hosts on target, and it comprises of various discoveries of the host such as TCP connections, ICMP ping and so on for scanning well known ports. The vulnerability assessment employs data aggregated.

Summary findings:

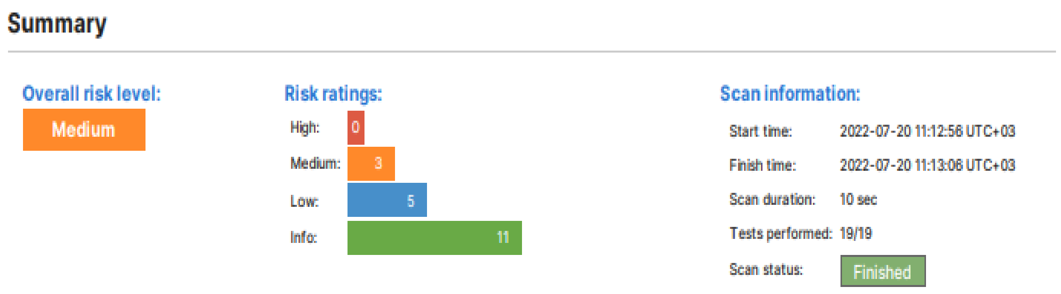
The results obtained from the audit process have been listed below and it is essential to scan the chosen link that is provided. The scanning results were provided and some of the listings that are provided below which has been obtained after scanning the network and they are:

- Insecure cooking
- Insecure configuration (Mamdouh, 2019)

The above findings shows that fewer risks only associated with this website, and it might affect accessing of the website.

Risk assessment:

The scanning was done and detected results were shown below. It has been found that the risks have been categorised on the basis of the severity level such as high, low and medium. The determination of the risks and their impact level can assure data integrity and security level. (Childs, 2021)



Summary

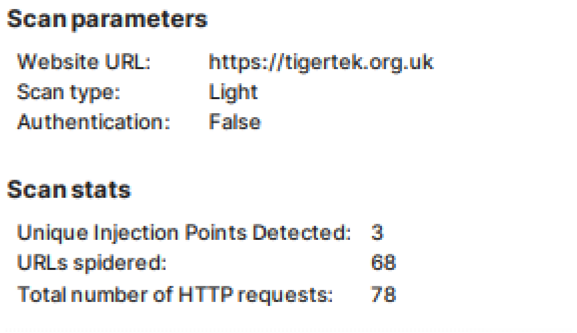
Overall risk level:
Medium

Risk ratings:

High:	0
Medium:	3
Low:	5
Info:	11

Scan information:

Start time:	2022-07-20 11:12:56 UTC+03
Finish time:	2022-07-20 11:13:06 UTC+03
Scan duration:	10 sec
Tests performed:	19/19
Scan status:	Finished



Scan parameters

Website URL:	https://tigertek.org.uk
Scan type:	Light
Authentication:	False

Scan stats

Unique Injection Points Detected:	3
URLs spidered:	68
Total number of HTTP requests:	78

The summary of the scan results was shown above, and thus suitable techniques must be adopted for the elimination of the risks that are identified.

Threat 1: Exposure of sensitive data

When a program does not safeguard sensitive information, a threat of this type can arise. Sensitive data may contain information about your finances, credit history, personal information, health information, etc. The main cause of it is inadequate encryption. The attackers take advantage of this circumstance and benefit in a few ways by using those personal details.

Impact of Vulnerability: High

Impact of Vulnerability Justification:

The attacker will have complete control and over database and will consequently incur a loss of money. Therefore, if student information is revealed, the university's reputation will suffer.

Medium - Level of Likelihood (Nageswara, 2014)

Probability Explanation

The likelihood of this attack is moderate, but if nothing is done to stop it, the victim will suffer significant harm. If the hackers take complete control, the severity of this risk will be very great.

Risk Degree: minimal

Risk Reduction

- Devices that require two factors for authentication can be used.
- Keys & passwords used only for authentication will be secure when strong password hashing methods like AES are employed.
- It is necessary to block autocomplete on forms when collecting sensitive data and cache for sites with sensitive data.

Threat 2 – Traffic analysis:

Vulnerability

In order to learn more about the communication patterns between the sender and receiver, network traffic is examined during the interception process. By using traffic analysis, it is possible to compromise the anonymity of the anonymous network. The smaller portions of intercepted data might be used by the attacker to identify patterns.

Impact of Vulnerability Level: High

Vulnerability Impact Justification

When the attackers discover a way into the information network with the help of communication patterns, the effect of this operation will be significant. The entire network may be impacted by the security breach, which will result in data leaking.

Likelihood Level: Low

Explanation for the Level of Likelihood

The university database has network monitoring tools installed, therefore the possibility of this kind of threat is limited. These technologies will effectively track network traffic, enabling excellent security.

level of risk – High

Risk Reduction

- To defend traffic analysis that takes place in networks, a dummy traffic approach might be built.
- Strong encryption techniques that mask communication patterns can get rid of these kinds of security risks.
- The network channel should be continuously monitored in order to spot assaults and take appropriate action.

Threat 3: An attack that steals cookies

Vulnerability

Using hacking tactics, the attacker will get access to the computer or network, and cookie theft will occur. It typically happens when a third party tries to copy unencrypted data and uses it to pretend to be the actual user. This kind of attack will develop whenever the user tries to access the trustworthy websites via an unsecured Wi-Fi network.

Impact of Vulnerability: Very high

Impact of Vulnerability Justification

Due to the unreliable websites, the vulnerability impact level would be very high and will result in customer dissatisfaction. Intruders can access the university database and change the data that is stored there by using cookie data.

Probability Level: Low

Because there is a significant chance that this attack may occur, the chances of it happening will be minimal. It implies that the burglars will carry out the operation using the ID and passwords. As a result, the cookies will be saved and not everyone will clean their browsing history.

Level of risk – High

Risk Reduction

- The web server will use SSL certificates, and the padlock will be activated. It will make sure that the server and browser have secure connections.
- Regular website updates can minimise numerous security risks because outdated software is a major cause of attacks.

Conclusion:

Attacks including denial of service, Trojan horses, equipment malfunctions, and software flaws can introduce a variety of invaders, leading to data breaches. The system's availability will be disrupted, making it impossible to deliver services to customers in a timely manner, thus leading to consumer unhappiness. The hackers will abuse the offered data by using the malicious code. Both administrators and users should maintain the secrecy of their passwords. If not, there will be many breaches. The testing were done and analysis of the threats were done and it is found that various threats such as website fingerprinting, common configuration issues and some of the cookie setting issues were level up.

Recommendation:

Corporate compliance must be adhered to in order to prevent misuse, legal repercussions, financial losses, and resource loss. The use of hard credentials can help to stop fraudulent actions. Additionally, 16-bit passwords are needed, which will entirely prevent any exploitation of the data in the software. It is necessary to implement strong control measures like a high security framework (Pahljina, 2018).

References:

Basit. (2011). Trivial model for mitigation of risks in software development life cycle. *International Journal of the Physical Sciences*.

Childs. (2021). Beyond the Dark Web: Navigating the risks of cannabis supply over the surface web. *Drugs: Education, Prevention and Policy*.

Maham. (2019). Security Issues in Software Defined Networking (SDN): Risks, Challenges and Potential Solutions. *(IJACSA) International Journal of Advanced Computer Science and Applications,*.

Mamdouh. (2019). Security Risks in the Software Development Lifecycle. *International Journal of Recent Technology and Engineering (IJRTE)*.

Nageswara. (2014). Identifying Risks and Possible Remedies to Mitigate Them during Systematic Software Development Process. *International Journal of Engineering Research & Technology (IJERT)*.

Pahljina. (2018). Mediating role of perceived benefits and risks of ict use in relation between approaches to teaching and ict teaching activities. . *EDULEARN18 Proceedings*.