An Overview of Information Security with Emphasis on Vulnerability Assessment Tools

VISHAL A. PAWAR[1], DR. MANOJKUMAR S. SONAWANE[2], DR. AMIT P. PATIL[3], CHHAYA S. PATIL[4], VITTHAL M. PATIL[5]

[1, 2, 3, 4, 5] *RCPET's Institute of Management Research and Development Shirpur*

Abstract- Any precaution taken to keep digital information and computer networks safe is included under the umbrella term "information system security." In the course of this investigation, a literature assessment of the significant background theory for the research subject was carried out. A comprehensive look at the research industry as a whole is presented, and the importance of developing preventative security technology is emphasised. When compared to the networks found in corporations, the ones found at colleges are exceedingly intricate. Nevertheless, it is required to keep up its already exceptional level of service. Security at universities can be difficult to maintain because to the vast number of users, the diverse client devices, and the academic freedom enjoyed by both academics and departments. It is possible for computer networks to go through a procedure known as scanning and vulnerability evaluation in order to ascertain the various types of security measures that have been implemented and the degree to which they are being attacked. It is essential to install screening and vulnerability assessment technologies in order to stop malicious software or hackers from exploiting security holes. This will prevent security flaws from being exploited.

Indexed Terms- Information security, Vulnerability, Vulnerability assessment tools, penetration Testing.

I. INTRODUCTION

Information system security may be defined as the process of securing data and information systems against unauthorized access, use, disclosure, interruption, alteration, and destruction. This definition comes from the CIA's triad of cyber security, which was developed in 2002.

Any action performed to protect the confidentiality of digital data and the integrity of computer networks is referred to as "information system security." It is a set of processes and technologies that are meant to keep computers secure from damage, whether that threat comes from within the network or from outside the network. System security refers to the measures taken by companies, organizations, and other types of institutions to safeguard their information technology (IT) infrastructure, data, and other types of digital assets, as well as to assure the dependability and consistency of their business operations.

Methods of information security that are successful at their jobs manage a wide range of threats and halt them in their tracks inside a safe and secure data network. It is required to set up a variety of checks and balances at the technical, structural, managerial, and operational levels in order to secure the privacy of individuals, the validity of information, and the accessibility of that information. For the sake of maintaining secrecy, it is necessary to prevent information from getting into the wrong hands and to restrict who may access it. Integrity refers to the protection of data from being altered in any way and the accurate permission of any data transfers that take place.

It has been proposed that all information security measures should begin with the CIA triad as their foundation. [Citation needed] (McCumber, 2005). Keeping information private, preserving trustworthiness, and ensuring that services are always available make up the CIA's "trifecta of assurance."

- Confidentiality- "ensuring that information is accessible only to those who are authorised to have access to it," as defined by ISO 17799, is the definition of confidentiality.
- Integrity - Integrity is "the activity of assuring the accuracy and completeness of information and

processing operations," according to the definition provided by the ISO-17799 standard.

- Availability - "ensuring that authorised users have access to information and associated assets when it is essential," is what the ISO-17799 standard defines as "availability." It is necessary to take steps in order to ensure the timely transmission of information and an ongoing flow of it in order to prevent enterprises from coming to a stop.

Another way to think about security in computer networks is that we try to safeguard the services and data from security threats.

II. NATURE OF INFORMATION SECURITY

According to Bishop (2003), regardless matter how effective the security measures are, the impact on a person's ability to maintain their privacy may be devastating if non-technical issues are not taken into account throughout the process of implementing and using the system. For instance, even the most well-designed security measures may be rendered ineffective and even deadly if they are installed or used negligently, giving birth to a false sense of security in the process. This can also give rise to a false sense of safety. It is advised in (Bishop, 2003) that knowledgeable architects, developers, and maintainers of security measures are vital to the successful application of such regulations in order to ensure that they are followed effectively. This includes every person who was involved, as well as the actions done to protect the mechanisms and the procedures that were followed. One of the most important variables is an individual's capacity as well as their awareness of how to respond responsibly in a precarious circumstance. Even the most up-to-date control methods cannot guarantee the security of the data. The degree to which users understand and are willing to comply with the requirements of security measures is typically a critical factor in determining how successfully a system is secured.

III. INFORMATION SECURITY ASSESSMENT AND VULNERABILITY ASSESSMENT TOOLS

The process of determining whether or whether an evaluated element (such as a host, framework, network, operation, or person) adequately achieves critical security objectives is known as information security assessment (or simply assessment) (NIST, 800-115). The remaining portion of (NIST, 800-115) provides an explanation of three separate evaluation methodologies that may be used to critically investigate cybersecurity: Tests, whether they be diagnostic or evaluative, as well as interviews and interrogations.

Scanning and vulnerability assessment is an in-depth investigation of computer networks that might reveal flaws in the defences protecting sensitive data. Because they monitor known security holes and analyse possible dangers before bad software or hackers can take advantage of them, screening and vulnerability assessment solutions are crucial. These resources serve as databases for vulnerabilities in networks and other mechanisms. In addition, it makes an effort to investigate each flaw in the services provided by the target host range and provides a grading of the flaw's severity in the final presentation. There are many such resources available, but our investigation zeroes in on three:

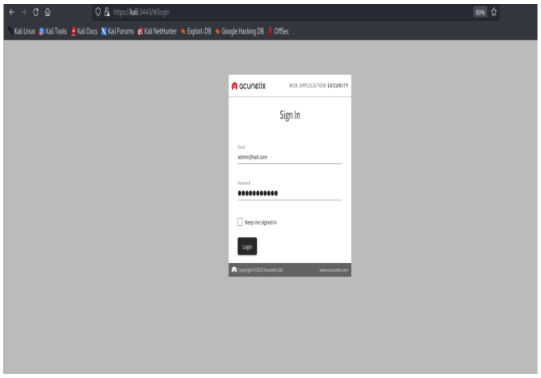
3.1.OpenVAS

OpenVAS, formerly known as Greenbone Security Manager, is a free and open-source vulnerability assessment system. Scan the network and applications for vulnerabilities using OpenVAS and get a report on the network's health.

An online vulnerability screening and management solution, OpenVAS is described as "a framework comprising numerous services and tools" (www.openvas.org)

3.2.Acunetix Vulnerability Scanner

Acunetix was the first of its kind in 2005 and has seen steady development ever since. It is an advanced, one-of-a-kind instrument developed by cybersecurity testing professionals.



Email: admin@kali.com

Password: ●●●●●●●●●●●●

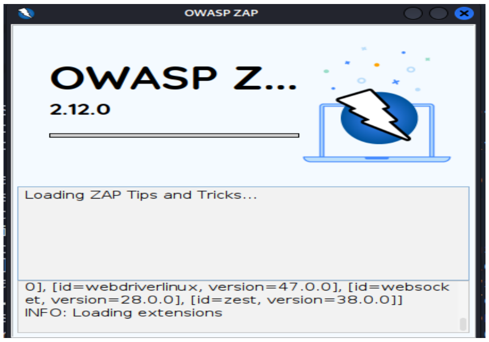
☐ Keep me signed in

Figure 1 :Accunetix Scanner

As a direct result of this emphasis, a workable alternative has been created that is superior in performance than the great majority of proprietary software. The Acunetix vulnerability scanner is a tool that may be used alone or linked into other systems to do comprehensive vulnerability testing on web applications. It is able to discover and manage vulnerabilities that are already known, for example, and works with a variety of features that are compatible with inexpensive software development tools. The addition of Acunetix to your security approach is a cost-effective solution to greatly boost your defences and remove many different types of attacks.

3.3.Zaproxy by OWASP

The OWASP Zed Attack Proxy (ZAP) is an easy integrated vulnerability scanner that may be used to locate security flaws in web applications. Although this tool was developed for researchers and professional testers who already have expertise with penetration testing, anybody who is interested in enhancing their security posture is free to use it.



```
Loading ZAP Tips and Tricks...
```

```
0], [id=webdriverlinux, version=47.0.0], [id=websock
et, version=28.0.0], [id=zest, version=38.0.0]]
INFO: Loading extensions
```

Figure 2: OWASP Scanner

CONCLUSION

This paper presents the literature review relevant to the research topic with respect to backgroundtheory. It includes a general review of significant work has been done in the research field andidentifyneed of preventivesecuritytechnologies. Universities have computer networks that are much more complicated than those in businesses. But it must keep giving the same high level of service to its customers. Universities can be hard to keep safe because of the large number of users, the different types of client computers, and the openness of an institution where teachers and departments work on their own. Scanning and vulnerability evaluation is a systematic look at computer networks and their parts to find out what security measures are in place and how much security is being attacked. Screening and vulnerability assessment solutions are important because they keep an eye on known security holes and look for possible threats before malicious software or hackers can use them. The information that these instruments gather is used to make a list of weaknesses in computer systems and other mechanisms. Its goal is to look into every problem with the services on the target host range and rate how bad they are before presenting the results. This research will help researchers to plan and conduct penetration testing. This will also help future researchers in designing a vulnerability mitigation plan for the vulnerabilities discovered in this study.

REFERENCES

[1] Yugansh Khera, et al. (2019), “Analysis and Impact of Vulnerability Assessment and Penetration Testing”, 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (Com-IT-Con), India, 14th -16th Feb 2019,IEEE.

[2] Shobha Tyagi, Krishan Kumar (2018),” Evaluation of Static Web Vulnerability Analysis Tools”, 978-1-5386-6026-3, 5th IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC-2018).

[3] Abhishek Raghuvanshi, Umesh Kumar Singh , Dr. Prashant Panse, Monika Saxena, “A Taxonomy of Various Building Blocks of

Internet of Things", International Journal of Future Generation Communication and Networking Vol. 13, No. 4, (2020), pp. 4397–4404

[4] Abhishek Raghuvanshi, Umesh Kumar Singh ,Chetan Bulla **,** Dr. Monika Saxena**,** Kishori Abadar **"**An Investigation on Detection of Vulnerabilities in Internet of Things**",** European Journal of Molecular & Clinical Medicine Volume 07, Issue 10, 2020, pp. 3289–3299

[5] Abhishek Raghuvanshi, Dr. Umesh Kumar Singh, Prashant Panse, Monika Saxena, Ravi Kishore Veluri , "Internet of Things: Taxonomy of Various Attacks", *European Journal of Molecular & Clinical Medicine*, *2020*, Volume 7, Issue 10, Pages 3853-3864.

[6] A. Raghuvanshi, U. Singh, T. Kassanuk and K. Phasinam, "Internet of Things: Security Vulnerabilities and Countermeasures", *ECS Transactions*, vol. 107, no. 1, pp. 15043-15052, 2022. Available: 10.1149/10701.15043ecst.

[7] Gurdeep Singh, Jaswinder Singh(2016)," Evaluation of Penetration Testing Tools of KALI LINUX", ISSN 2347 – 8616, International Journal of Innovations & Advancement in Computer Science IJIACS, Volume 5, Issue 9 September 2016.

[8] K. Pranathi , S. Kranthi , Dr. A. Srisaila , P. Madhavilatha (2018), "Attacks on Web Application Caused by Cross Site Scripting", Proceedings of the 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018), IEEE Conference Record # 42487; IEEE Xplore ISBN:978-1-5386-0965-1.

[9] Khochare and Dr. B. B. Meshram (2012),"Tools to detect and prevent web attacks", ISSN: 2278-1323, International Journal of Advanced in Computer Engineering & Technology Volume 1, Issue 4.

[10] [10] Fakhreldeen Abbas Saeed, Eltyeb E. AbedElgabar (2014)," Assessment of Open Source Web Application Security Scanners", ISSN: 1992-8645, Journal of Theoretical and Applied Information Technology, Vol. 61 No.2.

[11] Gabriela Roldán-Molinaa,b, Mario Almache-Cuevaa, Carlos Silva-Rabadãob, Iryna Yevseyevac, Vitor Basto-Fernandesb,d (2017)," A Comparison of Cybersecurity Risk Analysis Tools", Procedia Computer Science 121 , 568–575.

[12] Hessa Mohammed Zaher Al Shebli and Babak D. Beheshti (2018)," A study on penetration testing process and tools",2018,IEEE, Long Island systems, Applications and Technology Conference(LISAT)

[13] https://www.openvas.org/

[14] https://www.acunetix.com/vulnerability-scanner/

[15] https://www.zaproxy.org/

[16] Kachhwaha R., Purohit R. (2019) Relating Vulnerability and Security Service Points for Web Application Through Penetration Testing. In: Panigrahi C., Pujari A., Misra S., Pati B., Li KC. (eds) Progress in Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing, vol 714.Springer, Singapore.DOI:10.1007/978-981-13-0224-4_4.

[17] Touseef, P., Alam, K. A., Jamil, A., Tauseef, H., Ajmal, S., Asif, R., ...& Mustafa, S. (2019, July). Analysis of automated web application security vulnerabilities testing. In Proceedings of the 3rd International Conference on Future Networks and Distributed Systems (pp.1-8), DOI: 10.1145/3341325.3342032.

[18] Alanda, A., Satria, D., Mooduto, H. A., & Kurniawan, B. (2020, May). Mobile Application Security Penetration Testing Based on OWASP. In IOP Conference Series: Materials Science and Engineering (Vol. 846, No. 1, p. 012036). IOP Publishing.DOI:10.1088/1757-899X/846/1/012036.

[19] Yulianton, H., Trisetyarso, A., Suparta, W., Abbas, B. S., & Kang, C. H. (2020, July). Web Application Vulnerability Detection Using Taint Analysis and Black-box Testing. In IOP Conference Series: Materials Science and Engineering (Vol. 879, No. 1, p. 012031). IOP Publishing.DOI:10.1088/1757-899X/879/1/012031.

[20] M. Singh, P. Singh and P. Kumar, "An Analytical Study on Cross-Site Scripting," 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA),

Gunupur, India, 2020, pp. 1-6, doi: 10.1109/ICCSEA49143.2020.9132894.

[21] Z. C. S. S. Hlaing and M. Khaing, "A Detection and Prevention Technique on SQL Injection Attacks," 2020 IEEE Conference on Computer Applications (ICCA), Yangon, Myanmar, 2020, pp. 1-6, doi: 10.1109/ICCA49400.2020.9022833.