3rd National Level Students' Research Conference on "Innovative Ideas and Inventions in Computer Science & IT with Its Sustainability"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

A Study on Vulnerability Scanning Tools for Network Security

Asst. Prof. Dipali N Railkar[1], Prof. Dr. Shubhalaxmi Joshi[2]
[1]Research Scholar, Department of Master of Computer Application, MIT-WPU, Pune, Maharashtra, India
[1]Faculty, Department of Master of Computer Application, PCCoE, SPPU University, Pune, Maharashtra, India
[2]Associate Dean, Department of Master of Computer Application, MIT-WPU, Pune, Maharashtra, India

ABSTRACT

As world is moving towards complex networks and as we are moving towards digitization its value is increasing every day. Working of organization with internet and network is leading to the vulnerabilities. As we know for every organization data is an important feature and that need to be protected against the threats. Role of the Attackers is to use these vulnerabilities and try to exploit the networks. System security is one of the major aspects when organizations are working more with the support of Internet, intranet and associated techniques. Network security upholds computer systems from unwanted threats and intrusions which lead to reducing the risk of becoming victim to sensitive information theft. Preventing the systems and network from these vulnerabilities well in advance before attack happens will improve the confidence of the organization. For this organization must have proper network audits at place which is usually underestimated. There are various tools for Vulnerability Assessment is available for network audits and support for passive action to be taken to resolve those vulnerabilities. These tools can help organization to stop possible attack. In this paper we are showing the comparative study of Vulnerability Assessment tools for better clarity of the working of Cyber Défense Technology for enhancing security of network. The study conducted is relatively insightful, covering few features and parameters of network security and audit with respect to different tools like Nmap, Nessus, etc. It explores to learn that current tools need to be organized and with enhanced likely vulnerability coverage with respect to performance analysis. Finally, this paper is covering some challenges that existing vulnerability tools are facing towards network security.

Keywords — Vulnerability Assessment, Network Security, Network Audit.

I. INTRODUCTION

The world is getting increasingly connected because of the internet and new networking technology. Network security has received a lot of attention because of the open nature of the Internet. As new technologies emerge, businesses are moving their business processes to the cloud. A substantial amount of personal, economic, and organizational information is available via public networks on networking infrastructures all around the world. As a result, some precautions must be followed. Measures are taken to ensure that unauthorized persons are neither harmed nor unable to access the information. Unauthorized network access can be obtained by a third-party hacker or a disgruntled employee. Purposely injury or destroy secret data, causing a loss of profit and undermining the organization's capacity to compete in the marketplace. As a result, Network has gained a lot of grip is becoming increasingly critical due to the possibility of intellectual property theft. With a little effort and help from the internet one of the network security measures is scanning as well as Vulnerable Assessment and Penetration Testing (VAPT).[1-3] Computer systems and networks must be scanned to obtain information about their current state. Vulnerability scanning tools facilitate to identify vulnerabilities in different parts of network, devices, web services and applications. Whereas different static analysis tools used to find defects in code and audit tools can be used for finding different attacks on the system such as Trojan, root kit etc. The role of antivirus is to find the viruses, worms trying to damage the operating system or devices or applications. It's a technique for determining which hosts are active on a network with the goal of assessing network security. The word "vulnerability assessment" refers to the process of establishing one's security state of information systems through a systematic investigation. Both ways work well. The following services are provided for every organization's network: network auditing, penetration testing, reporting, and patching.

The importance of information and communication system security has raised to the top of the priority lists of both system developers and end users. On a daily basis, the dangers to our computer network architecture become more complex and sophisticated.[3,4] Attempts are being made by hackers to degrade or completely demolish our security system by conducting increasingly sophisticated attacks against a present vulnerability in our computer network system. It is necessary to train more cyber security professionals in order to defend our system and prevent cyber attacks. A key factor in the accomplishment of successful attacks, unreceptive offensive, and virus infections occurs when software vulnerabilities exist in computer systems, communication equipment, mobile phones, and other smart devices. An increasing number of cyber security courses are emphasizing offensive techniques such as buffer overflow attack and vulnerability exploits as opposed to exclusively defensive approaches such as encryption, intrusion detection, firewalls, and access control. It is vital to understand the many sorts of vulnerabilities that exist in computer systems before putting in place network defence measures. Therefore, vulnerability scanning is an important component of cyber security education. In the field of ethical hacking and network defence education, vulnerability scanning is one of the first procedures that must be taken. There are so many organizations that have made significant gains in the fields of automobile, electronics, physics, medicine, and applied sciences and other fields. These advancements, on the other hand, make them a prime target for hostile cyber attacks. [5, 6]

Confidentiality, integrity and availability are crucial when it comes to the sensitive data that higher education institutions manage (for example, intellectual property and financial information) (e.g., intellectual property, financial data). Because of the conflict between organizational culture, staffing, and resources, as well as the desire for effective security, businesses find it difficult to create and maintain effective security controls. [7] A considerable portion of the risk associated with enterprise network operations is accounted for by technical concerns such as software defects or misconfigurations. The use of standard vulnerability scanners (e.g., Nessus) on a regular basis can detect exploitable gaps in data-protection systems, allowing for the detection of exploitable weaknesses before they become a problem.

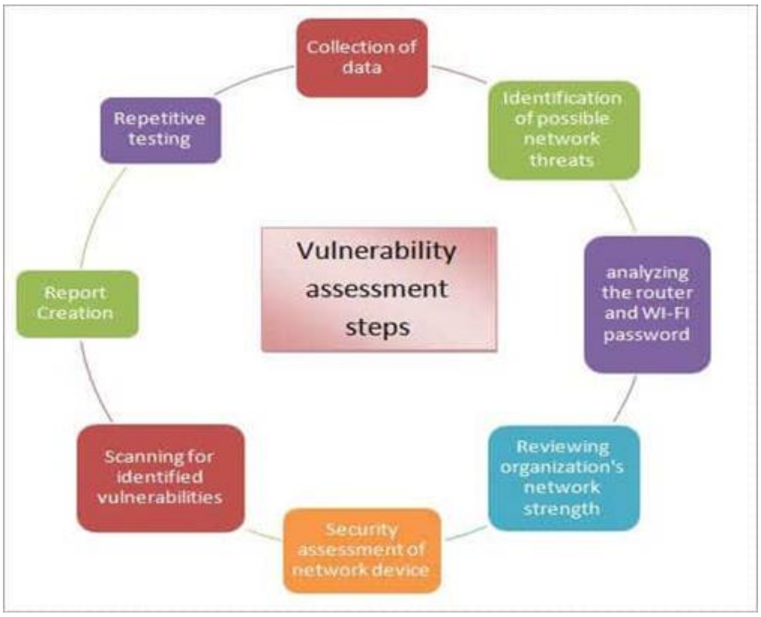
Collection of data
Identification of possible network threats
analyzing the router and WI-FI password
Reviewing organization's network strength
Security assessment of network device
Scanning for identified vulnerabilities
Report Creation
Repetitive testing
Vulnerability assessment steps

Figure 1- Network Vulnerability assessment steps

However, the security of the apps that are being migrated to the internet is a source of concern because it is directly tied to the security of the user who will ultimately use the programme. Finding software programme flaws that could risk the security of the user is therefore extremely important to ensure their protection. Identification of system faults prior to their being deliberately exploited to impose harm to the network is the goal of vulnerability assessment in information technology (IT). In this strategy, the vulnerability is detected and repaired before it is discovered and exploited by others, and it is used in combination with other techniques. Although the firewall has traditionally received more attention, internal functionality is as important. Vulnerability assessments are performed not only on a single application, but also on the platform, middleware, and operating system that the application is running on. It considers all of the variables that can lead to an accurate assessment of the system's vulnerability and security. In network systems and/or software applications, vulnerability scanners are tools that may be used to check for flaws in the system's operation.

There are two forms of scanning:

a) Inactive Scanning: Passive scanning utilizes the present network to determine whether a device is capable of detecting susceptibilities.

b) Active Scanning: Active scanning determines whether queries to the network for the vulnerability can be made.

The following are the various types of scanners:

i) Port Scanners: Using scanners, you can find out which ports are open and which ones are closed by scanning the ports. Also on their search list is information on the operating system and the services that are provided by the company.

ii) Application Scanners: It is necessary to scan a network application in order to detect vulnerabilities that could be exploited in order to compromise the entire system. Scanners for network applications are used to do this.

iii) Susceptibility Scanners: System flaws that could be exploited by a hostile user or hacker are sought after by violation scanners, which put the entire network system at risk of being hacked or otherwise compromised.

Through this paper we are focusing on the vulnerability scanning tools which are supporting to the network security. Aim of writing this paper is that individual as well as organizations are aware of different antivirus software and theses are commonly is practice for security. Vulnerability scanning tools are not extensively used in practice.

Further, this paper will support to select the proper vulnerability scanning tool as its features and coverage is varying according to different companies.

II. REVIEW OF EXISTING SURVEY ON VULNERABILITIES TOOLS FOR NETWORK SECURITY

Here author W. Alosaimi and colleagues throughout the current era of information technology, there are many new concepts to learn about, such as cloud computing, big data, the internet of things (IoT), and artificial intelligence. Customers and businesses are connected through a large number of service-related service information systems that were not designed specifically for this purpose by enterprises. [8]

Author W.M. Ma outlines information security attack and defence exercises in order to obtain a better understanding of the enterprise's external service information system. Internet penetration testing tool Hydra is well-known for identifying vulnerabilities in websites, and it is used by professionals to identify such problems. In the meantime, fresh investigators can obtain hands-on experience with website vulnerabilities, which will help them to improve their website penetration capabilities. [9]

In the research of WM Ma (William Ma) (2019) Even though they have significant limits in terms of scalability, functional engineering effort, and accuracy, old-style machine learning techniques have been frequently utilized in interruption discovery systems for years. Deep learning algorithms, which are particularly effective in the realm of enormous data, can be used to address these issues as a result of their efficiency. Deformation resistance and the elimination of the necessity for manual manufacturing are all advantages of deep learning. LSTM networks, as proposed by Diro and others, are used for dispersed network threat detection in the context of fog-to-object communication.[10] We discover and analyze important IoT device attacks and threats, focusing on the usage of wireless communication weaknesses. Experiments in two examples show that the depth model outperforms the classic machine learning model in terms of effectiveness and efficiency.

Work of Bailey C (2014)*et al.* presents trust-enhanced distributed authorization architecture as a holistic framework. When determining whether or not a platform can be relied on for permission, the technique considers both "hard" and "soft" concepts.[11] After providing an explanation of the reasoning behind the general model, the hybrid model with "hard" and "soft" trust components is detailed in further detail. Following that, the proposed architecture is put into action in the context of online service authorization. Specifically in a scattered situation, the findings indicate that the proposed technique facilitates more effective decision-making about permission. The authors of this paper investigate the possibility of authorization assets being automatically adapted to handle federated authorization infrastructures in the future (policies and subject access rights). SAAF (Self-Adaptive Authorization Framework) is a federated role/attribute management system that is based on policies for gaining access to and controlling authorization infrastructures. SAAF is a project of the National Institute of Standards and Technology.[10]

Here author R. Shanmugapriya et al. says due to the vulnerability of networks to denial-of-service attacks, security has garnered considerable attention. Although network administrators have taken every precaution to ensure network security, the system is sufficiently secure to conduct dispersion testing. This is the most efficient method of determining whether a system is vulnerable. Network security cybercrime technologies have brought a lot of positive things to the internet. With the most technological advancements, there is also a criminal hacker. [12]

Research work W. Alosaimi and colleagues presents an organization's exploits and vulnerabilities can be discovered through penetration testing, which is carried out on their computers. The information technology infrastructure contains security measures that contribute to the efficacy or ineffectiveness of the infrastructure. When weighed against the possibility of operational system failures, the greater expenditure in security controls makes more sense than previously thought. It is critical that penetration testing be carried out in a way that closely resembles a real-world attack.[13,14]

Focusing on the work of penetration testing L. Qing and his colleagues elaborate that a penetration tester rarely has the luxury of doing so, and a real-world attacker frequently spends months researching a target before launching an assault on it. All penetration tests are carried out in the same manner, regardless of whether or not an attack profile is being replicated in the laboratory. In order to acquire a target, the tester must first gather information about it. [15]

It is possible to create a natural mapping between discrete vulnerability measures and components from the larger spectrum of security skills under consideration, which includes: technical, user-oriented, and management-oriented security competencies. This can be accomplished using the CVSS version 3 framework. The CVSS score is used by the assessor to establish the level of vulnerability based on the information that is available at the time the assessment is performed. Among the CVSS Base metrics are the CVSS Base metrics (columns CVSS and Metric description), as well as the numerous values supplied by an assessor, which are summarised in Table 2. (Column Values) With the exception of the Scope metric, these are all of the metrics that the CVSS use in order to evaluate the severity of security vulnerability. [17-19] Here we have provided a brief summary of the technical abilities connected with the specific metric (Skill set), as well as a mapping of those technical abilities to the Knowledge Units defined by the American Computer Society's Joint Task Force on Cyber security Education.

Table1. A comparison of the susceptibilities noticed by several scanners is presented. [24]

Vulnerabilities	Nmap	Nessus	Acunetix WVS	Nikto	Burp Suite
SQL Injection	√	√	√		√
Inadequate Error Management.	√	√	√		√
Scripting on many sites.	√	√	√	√	√
Servers acting erratically	√	√		√	
Denial of Service	√	√	√		√
Execution of Code through the Internet.		√			
Identifier for the format string.		√	√		√
IIS printer		√	√		√

Table 2. Software vulnerability assessments are subjected to an accuracy evaluation.

CVSS	Metric Description	Values	Skill Set	Mapping
attack vector (AV)	The attack vector. The maximum distance an attacker can go to deliver an attack against a vulnerable component is indicated by this value. The higher the score, the greater the distance travelled.	Physical, Local, Adjacent Network.	As a result, the assessor is knowledgeable about the technical causes and attack vectors associated with software vulnerability. Among these include an awareness of susceptible settings, the delivery of local and remote attacks, and other aspects of the attack engineering process	Software Security: This course covers topics such as connectivity security (distributed system architecture, network services, and network defence); data security (data integrity and authentication, secure communication protocols); and network security (distributed system architecture, network services, and network defence).
Privileges Required (PR)	Required Privileges. Reflects the privileges required for an attacker to exploit the susceptible component on the affected system.	High, Low, None.	The assessor is well-versed in the relationship that exists between the vulnerable system, the user, and the attack, among other things. For example, spear-phishing efforts or users who do not pay attention to alerts.	The following subjects are discussed: Fundamental Principles, Implementation, Design, and Documentation of Software Security; Data Security: Data Integrity and Authentication.
Access Control (AC)	The difficulty of the attack. This indicates the presence of circumstances	High, Low.	local and remote attack delivery	Data Security: {Data Integrity and Authentication}

	that are required for the attack to succeed but are beyond the control of the attacker.			
User Interaction (UI)	Interaction with the User is important. The requirement for user engagement in order to launch a successful attack is represented by this symbol.	Required, None.	security problem over business transaction and data transmission	Data Security: {Data Integrity and Authentication}
Confidentiality (C)	Confidentiality. This method is used to determine the effect on the secrecy of information on the impacted system.	None, Low, High.	A security breach's impact on business-critical concerns such as data filtration and system performance can be quantified by assessors.	Software Security: {Deployment and Maintenance, Documentation, Implementation, Fundamental Principles}; Data Security: {Data Integrity and Authentication, Secure Communication Protocols}
Integrity (I)	Integrity. Calculates the implications of the impacted system's failure on the integrity of data stored on the impacted system.	None, Low, High.	Vulnerable systems for Remote healthcare monitoring Evaluation with real data.	Data Integrity and Authentication, Secure Communication Protocols are some of the terms used to describe data security.
Availability (A)	Availability. This function computes the impact on the component's availability.	None, Low, High.	interplay between a susceptible system, its user, and an intruding attacker	Software security covers a variety of subjects, including deployment and maintenance, documentation, implementation, and fundamental principles.

III. DISCUSSIONS AND FUTURE DIRECTION

In this part, the Susceptibility Valuation and Penetration Testing (VAPT) of many approaches are described in depth in Table 2 along with Figure 2. From the obtained data, it is obvious that the Partially Observable Markov Decision Process (POMDP), and Reinforcement Learning techniques beat the Mixed Initiative Planning and Scheduling Agent (MIPSA) and Host Clustering models in terms of accuracy. In addition, the POMDP and RL have identified the effective VAPT process over the other methods in a considerable way. Followed by, the POMDP technique has accomplished maximum confidentially over the other methods. Finally, all the compared methods have studied equivalent performance in terms of accuracy performance.[20-23]

Table 2 Performance Analysis (%) of Various VAPT Methods

Network Size	Accuracy Performance metrics (%)			
	POMDP	MIPSA	RL	Host Clustering
VAPT on 10 Machines	91.21	89.76	90.18	88.45
VAPT on 20 Machines	91.67	89.78	90.32	88.77
VAPT on 30 Machines	91.87	89.81	90.38	88.91

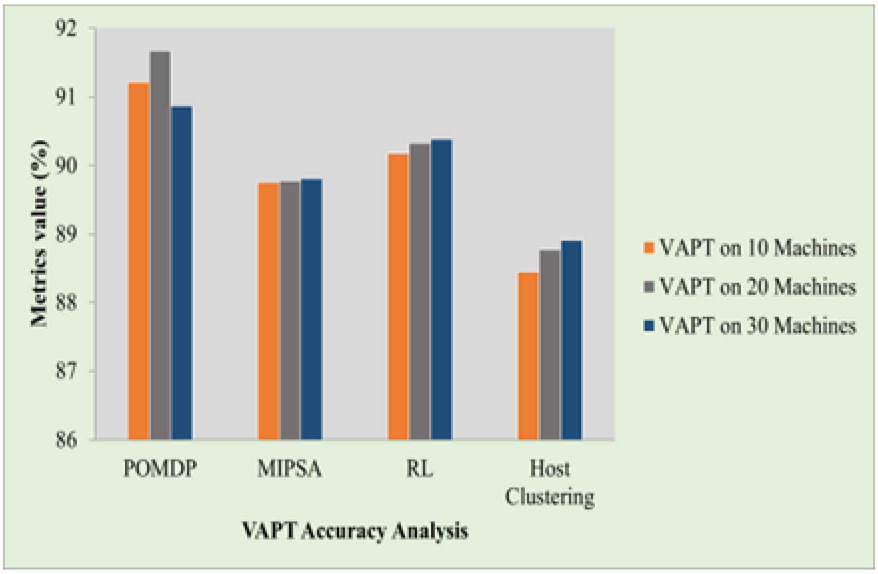

Fig.2 VAPT Accuracy Analysis of various methods

In Fig 2. For instance, the POMDP, RL methods have obtained higher accuracy of 91.21% and 90.18% for VAPT on 10 machines. whereas the MIPSA and Host Clustering methods have showcased lower accuracy of 89.76% and 88.45% for VAPT on 10 machines. Moreover, the POMDP and RL has resulted in maximum accuracy performance of 91.67% and 91.87% for the VAPT on 20 and 30 machines respectively. Finally, because VAPT continues to outperform the time typically allotted to PT experts on relatively large networks, we intend to improve on the current version by developing a hierarchical POMDP model of PT practice in which large networks are initially segmented (clusters) according to a security-oriented approach and the overall POMDP environment contains the cluster representation rather than a representation of all machines, as is currently the case. This technique is expected to address two critical testing challenges: performance optimization as a result of the system dealing with multiple small POMDP problems rather than a single large and complex environment, and reliability optimization as a result of the system dealing with multiple small POMDP problems rather than a single large and complex environment. A different approach is to use a hierarchical technique that simplifies and optimizes the process of gathering and processing information as attack vectors at two levels: clusters and future machines, and that can be applied at two levels: clusters and future machines, depending on how the network is modified.

IV. CONCLUSION

In this study, we specifically looked at how Vulnerability Assessment and Penetration Testing (VAPT) could be employed as a form of cyber defence against various threats with respect to network of organization. Here we have covered the brief idea of network vulnerability scanning process. We went over the entire life cycle of VAPT, as well as the most common VAPT approaches and the top vulnerability assessment tools. This Vulnerability Assessment and Penetration Testing, as well as their usage as a cyber defence technique, are covered in detail in this article. Paper focuses on the different techniques that are used by the researchers in the area of machine learning and deep learning. Basic comparison of the various vulnerability scanning tools with respect to performance analysis is elaborated. This gives a clear Idea that VAPT is an essential component of cyber defence and should be considered as such. This paper explains why increasing the use of VAPT is critical for total system security. Performance Analysis gives a clear idea that the development of new VAPT approaches and tools would be beneficial for better scanning in a less duration with increased number of system or machines. This status of the paper VAPT is a cutting-edge cyber-defence technology. Compulsory VAPT testing can help prevent cyber-attacks in the future as well as bolstering network security.

V. REFERENCES

[1]. Wu YX, Wang HF. Computer network information security risks and protective measures against the background of big data. J Luohe Vocat Tech Coll. 2019;4:20–2.

[2]. Xiao-Xia W. Research on information security architecture of computer network. Digital Technol Appl. 2018;36(12):181–2.

[3]. Harshdeep Singh, Dr.Jaswinder Singh, “Penetration testing in wireless networks”, International Journal of Advanced Research in Computer Science, 8 (5), May-June 2017, pp. 2213-2216 .

[4]. Dongying L, Baohai Y. Research on information security strategy based on wireless network access. Digital Technol Appl. 2018;36(11):191–2.

[5]. Prashant S. Shinde, Prof. Shrikant B. Ardhapurkar, “Cyber Security Analysis using Vulnerability Assessment and Penetration Testing”, Presented at IEEE Sponsored World Conference on Futuristic Trends in Research and Innovation for Social Welfare (WCFTR’16), 2016.

[6]. Wang, Yien, and Jianhua Yang. "Ethical hacking and network defense: Choose your best network vulnerability scanning tool." 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA). IEEE, 2017

[7]. Harrell, Christopher R., et al. "Vulnerability Assessment, Remediation, and Automated Reporting: Case Studies of Higher Education Institutions." 2018 IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE, 2018.

[8]. Alosaimi W, Zak M, Al-Begain K, Alroobaea R, Masud M. Mitigation of distributed denial of service attacks in the cloud. Cybern Inf Technol. 2017;17(14):32–5.

[9]. Ma WM. Research on website penetration test. Glob Bus Manag J. 2019;11:121–32.

[10].Wang, Liwei, Abbas, Robert, Almansour, Fahad M., Gaba, Gurjot Singh, Alroobaea, Roobaea and Masud, Mehedi. "An empirical study on vulnerability assessment and penetration detection for highly sensitive networks" Journal of Intelligent Systems, vol. 30, no. 1, 2021, pp. 592-603. https://doi.org/10.1515/jisys-2020-0145

[11].Bailey C, Chadwick DW, de Lemos R. Self-adaptive federated authorization infrastructures. J Comput Syst Sci. 2014;80(5):935–52.

[12].Shanmugapriya R. A study of network security using penetration testing. 2013 international conference on information communication and embedded systems (ICICES). IEEE; 2013, February. p. 371–4.

[13].Alosaimi W, Zak M, Al-Begain K, Alroobaea R, Masud M. Economic denial of sustainability attacks mitigation in the cloud. Int J Commun Netw Inf Security. 2017;9(3):420–4314.

[14].Alosaimi W, Zak M, Al-Begain K, Alroobaea R, Masud M. Mitigation of distributed denial of service attacks in the cloud. Cybern Inf Technol. 2017;17(14):32–5.

[15].Qing L, Boyu Z, Jinhua W, Qinqian L. Research on key technology of network security situation awareness of private cloud in enterprises. In 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA). IEEE; 2018. pp. 462–6

[16].Allodi, L., Cremonini, M., Massacci, F. et al. Measuring the accuracy of software vulnerability assessments: experiments with students and professionals. Empir Software Eng 25, 1063–1094 (2020). https://doi.org/10.1007/s10664-019-09797-4

[17].Kyriakos Kritikos *, Kostas Magoutis, Manos Papoutsakis, Sotiris Ioannidis .A survey on vulnerability assessment tools and databases for cloud-based web applications. www.elsevier.com/journals/array/2590-0056/open-access-journal. https://doi.org/10.1016/j.array.2019.100011

[18].Jai Narayan Goela, B M Mehtre Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. Peer-review under responsibility of organizing committee of the 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015) doi: 10.1016/j.procs.2015.07.458

[19].Sowmyashree A, Dr. H S Guruprasad, "Evaluation and Analysis of Vulnerability Scanners: Nessus and OpenVAS" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

[20].Mohamed C. Ghanem ,Thomas M. Chen "Reinforcement Learning for Efficient Network Penetration Testing" Information 2020, 11, 6; doi:10.3390/info11010006 www.mdpi.com/journal/information.

[21].Jonathon Schwartz, Hanna Kurniawati "Autonomous Penetration Testing using Reinforcement Learning", arXiv.org- cs- arXiv:1905.05965

[22].Zhenguo Hu, Razvan Beuran, Yasuo Tan, "Automated Penetration Testing Using Deep Reinforcement Learning" 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)

[23].Dean Richard McKinnel, Tooska Dargahi, Ali Dehghantanha, Kim-Kwang Raymond Choo, A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability

assessment, Computers & Electrical Engineering, Volume 75,2019,Pages 175-188, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2019.02.022.

[24].Sheetal Bairwa, Bhawna Mewara and Jyoti Gajrani Vulnerability Scanners-A Proactive Approach To Assess Web Application Security Article in International Journal on Computational Science & Applications · March 2014 DOI: 10.5121/ijcsa.2014.4111 · Source: arXiv