CYBER ATTACK PREVENTION USING VAPT TOOLS

G Swaroop, *Student*
Dept. of Computer Science and Engineering
Atria Institute of Technology
Bangalore, India
swaroopg619@gmail.com

Harish Budarpu, *Student*
Dept. of Computer Science and Engineering
Atria Institute of Technology
Bangalore, India
harishbudarpu@gmail.com

Manasa B N, *Student*
Dept. of Computer Science and Engineering
Atria Institute of Technology
Bangalore, India
manasabn656@gmail.com

Prof. Meghashree N, *Assistant Professor*
Dept. of Computer Science and Engineering
Atria Institute of Technology
Bangalore, India
1meghashreenagesh@gmail.com

Abstract— **Networks and systems lack sufficient security and are prone to numerous types of cyber security threats. In the past, we've witnessed a major increase in cyber- attacks. Such situations lead to agendas called cyber security and cyber-attack prevention of public and personal networks. The process of identifying the vulnerabilities in the systems and networks is called as Vulnerability Assessment. Vulnerability Assessment helps in providing necessary solutions to mitigate risks. This involves identification of vulnerabilities, the assessment amongst the dangers associated with the vulnerabilities, and the provision of the necessary solutions. The process must be executed in a manner that is consistent with organizational guidelines and practices and with the security objectives of a system. It must take place on a regular basis to ensure the safety of the systems and networks.**

Keywords: cyber security, cyber-attack prevention, vulnerability assessment, penetration testing.

I. INTRODUCTION

Cyber-attacks can be defined as a series of actions that are performed by people who typically use malicioussoftware to gain entry to a person's or organization's computer or network. They can also cause malfunctioning of computer systems, resulting in loss of data, system crashes, and decreased performance. Cyber-attacks can be performed by one individual or a group from any given location. Those who launch these types of cyber-attacks are called cybercriminals or hackers

II. TYPES OF CYBER ATTACKS:

1. Ransomware - Ransomware is a type of malicious software that locks down a computer or mobile device and blocks permission to the user's data until a ransom payment is made. The attacker usually demands a payment to unlock obtained data and release the device. It is of the utmost importance to take precautionary measures to shield oneself from ransomware attacks, such as backing up your data regularly and using strong passwords.

2. Malware: Malware can be used to compromise online content, steal data, or harm a computer system. Botnet malware, cryptocurrency miners, information thieves, and banking mobile malware Trojans are a few common types.

3. DoS and DDOS Attacks: Distributed denial-of-service attacks are multiple host machines. They are used for sabotaging security teams while attackers can perform the attacks. These attacks bombard a web server or any other type of computer system via a large number of requests, overwhelming the system and preventing it from processing legitimate requests.

4. Phishing and Social Engineering Attacks: Social engineering can be defined as an attack that relies on human interaction and the same is applied over 90% of cyberattacks. This can involve cases like impersonating any trusted person and tricking them to grant their sensitive information or provide access to their systems.

5. MitMAttacks: Man-in-the-Middle attacks enable the attacker to intercept, alter and even replace the data that is being transmitted from one party to another. The attacker can also eavesdrop on the communication taking place. This attack can be employed to gain admission to private information such as usernames, passwords and data.

III. LITERATURE SURVEY

[1] Grusha Kaur Sahni and Ravindranath Kongara used an approach called STAAS, which comprises of five modules and assists in the detection of application vulnerabilities. These vulnerabilities must be tested in a system or network. This technique helps security engineering by enhancing any team's resources and risk visibility. It assists in the integration of solutions, increases accuracy, and speeds up software testing.

[2] Vivek Shrivastava and Monika Pangaria state that the main goal is to test certain vulnerabilities using the well- known sand penetration testing programs, Accunetix and waf, before comparing them in terms of case of use, resource usage, and

processing speed. While w3af is well- known for its auditing capabilities, it was discovered that accunetix has considerably greater reporting capabilities.

[3] Catalin Mironeamu and Alexandru Archip suggested the Experimental Cyber Attack Detection Frame-work. This architecture was created particularly to facilitate on- the-fly secure research. This could be carried out by combining the offline data to real time traffic study, which can also aid in determining the kind of legally permissible
network access.

[4] Pranjal Chowdhury and Sourav Paul created a technique that aids in the discovery of cyber-attacks by utilizing three attacks: Zero, Hybrid, and Fault. These cause any sort of cyber system to fail, and it's been discovered that higher corruption and larger web information measure the attacks beginning.

[5] Dmitry Zegzhda and Daria Lavrova presented an evolutionary strategy that incorporated two major components. First, a machine learning algorithm is used to discover patterns and trends in the history of previous security occurrences. Second, evolutionary models are used to mimic the growth of countermeasures in observed flaws.

[6] Diego Mena Baijian Yang Mendez developed a proof of concept (PoC) for the use of blockchain technology. A distributed network of cyber threat intelligence information exchanges was established using blockchain technology, with each node holding its own transaction data and cryptographically protected transactions. ISPs, home networks, and home-based IoT devices may all safely and effectively share cyber threat intelligence data thanks to this distributed network.

[7] Jorg Schwenk and Christian Mainka presented a web service attacker tool to aid in the improvement of a framework for web service specialized plugins. It aids in the dissemination of information concerning Web Service Specific Non-Specific Attacks, SOAP Action Spoofing, and WS-Addressing Spoofing. This suggested framework indicates regardless if the assault was successful and also offers an evaluation of the attack's impact.

[8] Zoran URI proposed a system that uses a web crawler to collect data and an EAP detector and extractor, followed by an attack generator and analyzer module that consists of SQLI, XSS, and BOF to secure the website using their own algorithm issued by the three different tools, and finally providing a vulnerability report.

[9] N. Antunes and N. Laranjeiro proposed an automated method for finding SQL Injection and XPath Injection issues. The approach entails intercepting every SQL or XPath instructions that are performed, generating a workload, and learning SQL and XPath statements from the service. The attack load is run to detect vulnerabilities considering the workload generation of SQL Injection and XPath Injection attacks. To find vulnerabilities in online services, the tool Command Injection Vulnerability Scanner for online Services is utilized.

[10] According to Xiaowei Li and Yuan Xue, when client-side code is exposed, the aggressor has data about the program and hence has greater vulnerabilities. According to the research, we may improve security by addressing security concerns at their source (which is the most dependable), verifying (dynamic analysis and cross checking), and protecting (creating a safe software).

[11] Jai Narayan Goe, BM Mehtre, discusses how vulnerability assessment and penetration testing may be applied efficiently. Because there are numerous open- source premium tools for Vulnerability Assessment and Penetration Testing Tools (Metasploit, Nessus, BurpSuite, w3af, OpenVAS Appscan, Kalilinux). VAPT testing should be mandatory to avoid cyber-attacks and increase system security.

[12] Pranav Nerurkar, Aruna Pavate, and Pranav Nerurkar demonstrate in detail how to utilize various tools and how they operate and are correct. The data could be utilised to select the most appropriate penetration testing instrument. They utilized Autopwn to examine the browser's vulnerability for the Metasploit framework. Using these techniques, they discovered vulnerabilities such as SQL injections, XST, and XSS issues.

[13] Larisa Gabudeanu and Mircea Constantin Scheau supported a risk-based strategy based on data collecting and statistical analysis of attack techniques and countermeasures. The analysis will define the requirements required to carry out risk assessment processes to prevent malware attacks on mobile banking systems. This proved that, although certain cyber assaults may be resolved by payment service providers, others need alerting clients of the existence of malware.

[14] J.P. McDermott recommended that a bug be defined as an accurate and succinct statement of an undocumented security vulnerability. The results show that it is quite helpful to model penetration testing as a Petri net. While adding a few new benefits, it preserves the primary benefits of attack tree approaches and the defect hypothesis.

[15] According to Alberto Acosta López, Elver Yesid, wireless network protocols have become out-of-date as a result of the emergence of new intrusion tactics and technology. The study sought to judge the safety of the commonly used WPA2. The security of the protocol was also rated using Linset and Aircrack-ng, two wireless system auditing tools.

[16] According to Elyas Baray and Nitish Kumar Ojha, wireless networks and Wi-Fi-based technologies pose a substantial danger to data security. The discussion covers a variety of security model problems, such as Aircrack- ng's hacking of Wi-Fi security, holes in previous security models, and the effectiveness of the Aircrack-ng assault on Wi-Fi modems and routers. Many businesses attempt to address security flaws in the absence of security solutions. The device can connect to

incompatible devices by downgrading from WPA3 to WPA2, which is a problem due to the new WPA3 protocol.

[17] Jay Narayan Goel describes how systems are becoming increasingly complex. As a result, systems become increasingly vulnerable. These flaws allow attackers to get access to the victim's machine. It is preferable to discover these problems before an attacker does. Although penetration testing and vulnerability assessment may be utilized to offer proactive cyber protection, their use is often overlooked. It has been demonstrated in this study that the cyber security method known as vulnerability assessment, in conjunction with penetration testing, become accustomed to provide active cyber defense.

[18] Prashant S.Shinde and Shrikant B.Ardhapurkar proposed a diversity of penetration testing and vulnerability assessment techniques (VAPT). Organizations should start by putting in place a comprehensive security strategy that incorporates both technological and non-technical safeguards. Identifying identification and access control, encryption, and the usage of secure protocols should all be considered technical precautions. Non-technical measures such as personnel training, policy enforcement, and regular security assessments should also be implemented by organizations.

[19] Deepansh Kumar, Yugansh Khera, describes how the fast growth of mobile and computer systems has resulted in the development of more complex and effective Windows, Web, and mobile apps. Vulnerability and penetration testing processes enable it to determine if the security system's arrangements are effective or not by solving security gaps.

[20] According to Sugandh Shah and B.M. Mehtre, the Internet's capacity to allow firms to transmit information internationally has produced a limitless number of chances. It has, however, exacerbated security dangers and cyberthreats. It helps enterprises to apply fixes and execute appropriate security precautions in order to defend themselves from future threats. A brief explanation of the methodologies and processes employed in VAPT, as well as its benefits and safety measures

[21] Michael K Kissi and Michael Asante elaborate on how the widespread adoption of wireless networks, driven by their flexibility, mobility, and simplicity, has led to their ubiquitous use in various settings such as restaurants, hotels, airports, businesses, and homes. However, this convenience comes with risks, as attackers can intercept data packets easily when multiple devices connect to these networks, potentially exposing sensitive information. This study focuses on testing the shortcomings of Wi-Fi Protected Access (WPA) and Wireless Equivalent Privacy (WEP) security protocols. The researchers conducted pen testing using Kali Linux and its Aircrack-ng tools to identify weaknesses in these protocols.

[22] Shree Lamichhane illustrates the security protocols and techniques employed in encrypting and decrypting data during wireless network transmission. The study explores prevalent security threats in wireless networks and outlines the evolution of the popular IEEE 802.11 standard along with its amendments. Furthermore, it showcases the vulnerability of a WPA-secured network, revealing how it will be cracked effortlessly using Kali tools.

[23] K Sinchana and C Sinchana assert that the abundance of data generated due to internet innovations, e-commerce applications, and social networks poses challenges for secure transmission over the internet. Network security solutions play a crucial role in safeguarding Wi-Fi networks, securing websites and online applications against vulnerabilities, password cracking, and ensuring message encryption. The paper introduces various tools addressing network scanning, protocol analysis, network security, and website vulnerability analysis.

[24] Aswin Raghuprasad and Suraj Padmanabhan proposed a system that outlines common attack methods, explaining their functioning, and emphasizes prevention as an additional security measure for IoT devices. The suggested system effectively thwarts a range of attacks, particularly those utilizing MAC addresses to target victim IoT devices, including DoS and DDoS attacks.

[25] Vasaka Visoottiviseth and Phuripat Akarasiriwong proposed a PENTOS penetration testing system designed specifically for IoT devices. PENTOS, operating through wireless connections like WiFi and Bluetooth, autonomously gathers data from the targeted IoT device. Users can employ the system to assess vulnerabilities in their IoT devices, employing techniques such as password attacks, online attacks, and wireless attacks to gain privileged access. Following the penetration testing, the system presents results from all attacking modules and provides recommendations for secure deployment to guard against potential attacks.

[26] Eric B. Blancaflor and Luis Antonio Alvarez assess the vulnerability of default settings in SOHO Routers provided by public/private communication companies to their customers. The study also examines the insufficient or outdated protection mechanisms employed by these routers. Using Kali Linux, the research tests the routers' susceptibility to network attacks.

[27] E Budi Setiawan and Angga Setiyadi clarify that a website and a computer network interconnected with each other hold equal importance concerning data security on the internet. In the realm of computer networks, any data on one computer linked to another is vulnerable. Hence, it is essential to implement measures to safeguard this data from being accessed or viewed by other computers.

[28] John Mark Weber and Frederick T. Sheldon provide examples of how ubiquitous Wi-Fi is as the most widely utilized wireless network protocol. WPA's release in November 2008 made it possible to spoof Address Resolution Protocol (ARP) packets. The basis of this research is a specific categorization of Wi-Fi attacks, modifications to current countermeasures, and protocol changes.

[29] According to ME Elhamahmy, Tarek S. Sobh, there is a serious problem with information leakage in today's extensively used Wi-Fi networks. War-Driving attacks are a serious issue because they compromise regularly used wireless network hosts and result in data leaks. The suggested approach provides an open-source software- based customized tool. It makes an effort to prevent data from leaking from a computer connected with a Wi-Fi network. The trials, which also involve the War-Driving attack, employ an attack scenario to evaluate the effectiveness of the propose tools.

[30] Vincent Tran and Jesus Nunez discuss how the increasing use of drone technology has made it a preferred option for businesses to use for certain tasks. The growth in popularity has led to a rise in the significance of security analysis. We will also examine the current security protocols and auto-pilot systems for vulnerabilities and common network system cyberattacks. Other forms of attacks are also looked into to see if there are any more attack vectors that could jeopardize the system beyond interfering with the drones' network connectivity.

[31] Kajal Kashyap and Arti Noor present an overview of numerous open-source penetration tools featured in Kali Linux. The research delves into the analysis and comparison of these tools, considering their utility and portability. Additionally, it delivers a detailed, step-by- step guide on how to utilise each penetration testing tool.

[32] According to Johanna Janse van Rensburg and Barry Irwin, 802.11 wireless networks' security vulnerabilities have drawn a lot of attention in recent years. This study discusses and assesses software, both open-source and commercial, that is applied to map, analyze, secure, and audit wireless networks. The functions of each tool will be grouped corresponding to the roles that they each perform.

[33] J Keiny and Grau Ortiz provides support for a newly created tutorial that focuses on different approaches to penetration and vulnerability exploiting. Those who utilize these tools can assess any network's dependability. This article provides a brief description of each tool's attributes along with some examples of possible outcomes.

[34] Ömer Aslan and Refik Samet provided numerous penetration testing methods that leveraged the Nmap and Metasploit frameworks to find vulnerable hosts and applications. A virtualized system running multiple Linux and Windows OS versions is used as a test case.

[35] Ömer Aslan advised that the problem of cyberattacks persists even with the release of patches for existing operating systems (OSS) and application software vulnerabilities. A thorough approach to penetration testing is employed to tackle this problem, with a particular focus on locating susceptible hosts and applications using programs like Nmap and the Metasploit framework. Numerous tools in the Kali Linux OS are helpful for identifying vulnerabilities. These include the well-known Nmap, Metasploit framework, Wireshark, John the Ripper, Ettercap, and Burp Suite.

[36] Azaz Ahamed and Nafiz Sadman compiled a group of the ten most crucial security flaws that need to be monitored and addressed to ensure safer internet connectivity. They conducted thorough testing using tools such as Burp Suite, ZAP, and Net sparker to identify recurring vulnerabilities in various web application sections. These tools were compared and evaluated across web applications in their respective industries, and the findings were presented accordingly. The research revealed that the services and transportation sectors were particularly vulnerable to these security issues.

[37] Ömer Aslan presented a three-step method that includes feature selection, identification, and preprocessing. Features that weren't required for the model was eliminated through preprocessing. Using procedures like Gain Ratio, Information ratio, Correlation Coefficient, the most important elements were chosen. The number of features was reduced from 87 to 20. Different classifiers were employed to distinguish between DDoS attack.

[38] Bitlis Eren, from Bitlis Eren University, proposed a technique that involves analyzing ransomware actions performed on file. The locations where these behaviors occurred were assigned weights. By considering these weights and Information Gain, features with the highest likelihood of success were selected. ML classifiers like RF, KNN, BN, SMO classified selected features, tested on various ransomware versions and safe samples.

[39] Ömer Aslan and Abdullah Asım Yılmaz introduced a fusion architecture aimed at enhancing the integration of two distinct pre-trained network models. The architecture involved four key steps: data collection, designing a deep neural network structure, training the proposed network, and evaluating its performance. Test results demonstrated the effectiveness of this approach in accurately categorizing malware.

[40] A malware analysis system using two methodologies was presented by Ömer Aslan and MERVE OZKAN- OKAY. The client submits samples of suspicious files to the cloud for evaluation, and then receives the findings to determine whether the samples include malware. The system examines file samples with specific tools to collect execution traces from several virtual machines.

IV. EXISTING SYSTEM

The inclusion of an extensive amount of code into the process introduced complexities. It became crucial to determine a tool that offered superior accuracy, speed, and memory efficiency. The reliance on outdated individual tools proved unreliable, necessitating to look for a solution with enhanced performance. Maintaining the code base became challenging, leading to prolonged testing and examination of the platform.

V. PROPOSED SYSTEM

This idea offers a vulnerability scanner that can locate the ideal level of security needed by an individual or organization. Utilizing VAPT tools, cyber-attack prevention is implemented to achieve this. By doing this, we'll be able to see any vulnerabilities within a framework or network and fix them before they work against us. The suggested system contains a wide range of tools to look for any weaknesses or openings. The methods employed would be cutting-edge and highly accurate. The system can spot any kind of weakness or opening. The suggested system will be simple to operate.

VI. CONCLUSION

A vulnerability scanner is a means that can help groups and individuals protect their systems and networks from cyber-attacks. It works by identifying and fixing vulnerabilities before they can be exploited by attackers. VAPT tools are a kind of vulnerability scanner which could be utilized to test a broad variety of systems and networks, including web applications, networks, and operating systems. VAPT tools can identify various vulnerabilities, such as common vulnerabilities and exposures (CVEs), web application vulnerabilities, and network vulnerabilities.

REFERENCES

[1] Ravindranath Kongara, "vSTAAS - an Integrated Pen-Testing Tool", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019.

[2] Monika Pangaria, Vivek Shrivastava, Archita Bhatnagar, "Comparative Study of Web Application Penetration Testing Tools", Intl Conference on Electrical, Electronics and Computer Science (ICEECS).

[3] Catalin Mironeanu ,Alexandru Archip, "Experimental Cyber Attack Detection Framework",July2021,Electronics 10(14):1682, DOI:10.3390/electronics10141682

[4] Pranjal Chowdhury, Sourav Paul, "Cyber-Attack in ICT Cloud Computing System", January2023, DOI:10.1007/978-981-19-0095-2_12.

[5] Dmitry Zegzhda, Daria Lavrova, "Cyber Attack Prevention Based on Evolutionary Cybernetics Approach" 2020, 12(11), 1931; https://doi.org/10.3390/sym12111931

[6] Diego Mendez Mena,Baijian Yang,"Decentralized Actionable Cyber Threat Intelligence for Networks and the Internet of Things"

[7] Christian Mainka, J¨org Schwenk, "Penetration Testing Tool for Web Services Security", June 2012.

[8] Zoran ĐURIĆ, "WAPTT - Web Application Penetration Testing Tool", Advances in Electrical and Computer Engineering 14(1):93-102.

[9] N. Antunes, N. Laranjeiro, M. Vieira, H. Madeira, "Effective Detection of SQL/XPath Injection Vulnerabilities in Web Services", IEEE SCC 2009, pp. 260-267, 2009.

[10] X. Li and Y. Xue, "A Survey on Web Application Security", Technical report, Vanderbilt University, 2011.

[11] Analysis and Evaluation of Wireless Network Security with the Penetration Testing Execution Standard(PTES) by Deuis Nur Astrida, Agung Restu Saputra and Akhmad Ikhza Assaufi.

[12] Aruna Pavate, Pranav Nerurkar, "Performance Analysis of Cloud Based Penetration Testing Tools", International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue

[13] Mircea Constantin Scheau,Larisa Gabudeanu,"Risk-based approach in preventing mobile banking cyber-attacks"Conference: 25th RSEP International Conference on Economics, Finance & Business,At:Paris, France;Volume: ISBN: s978- 605-70583-8-6

[14] J.P.McDermott,"McDermott, J. P. Assault net penetration testing. Within Proceedings of the 2000 workshop on New security paradigms (pp. 15-21).

[15] Alberto Acosta López, Elver Yesid,"Evaluation of WPA2-PSK wireless network security using the linset and aircrack-ng tools,Facultad de ingeniería 27(47),71-78,2018

[16] Elyas Baray, Nitish Kumar Ojha,"WLAN security protocols and WAP3 security approach measurement through aircrack-ng technique",2021 5th Global Conference on computing Methodologies and communication (ICCMC), 23-30,2021

[17] Jai Narayan Goel,"Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology" Procedia Computer Science 57 (2015) 710 – 715

[18] P. S. Shinde and S. B. Ardhapurkar, "Cyber security analysis using vulnerability assessment and penetration testing.

[19] Y. Khera, D. Kumar, Sujay and N. Garg, "Analysis and Impact of Vulnerability Assessment and Penetration Testing," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon),2019 pp. 525-530, doi: 10.1109/COMITCon.2019.8862224.

[20] Sugandh Shah, B.M. Mehtre,"A Modern Approach to cyber security analysis using vulnerability assessment and penetration testing, International journal of electronics communication and computer engineering: Volume 4, Issue(6).

[21] Kissi, Michael K., and Michael Asante. "Penetration testing of IEEE 802.11 encryption protocols using Kali Linux hacking tools." International Journal of Computer Applications 975 (2020): 8887.

[22] Lamichhane, Shree. "Penetration Testing In Wireless Networks." (2017).

[23] Sinchana, K., Sinchana, C., Gururaj, H. L., & Kumar, B. S. (2019, July). Performance evaluation and analysis of various network security tools. In 2019 International Conference on Communication and Electronics Systems (ICCES) (pp. 644-650). IEEE.

[24] Raghuprasad, A., Padmanabhan, S., Babu, M. A., & Binu, P. K. (2020, July). Security analysis and prevention of attacks on IoT devices. In 2020 International Conference on Communication and Signal Processing (ICCSP) (pp. 0876-0880). IEEE.

[25] Visoottiviseth, V., Akarasiriwong, P., Chaiyasart, S., & Chotivatunyu, S. (2017, November). PENTOS: Penetration testing tool for Internet of Thing devices.

[26] B. Blancaflor, E., Alvarez, L. A., Dionisio, N. M., Acuna, G. E., Funilas, J. R., & Odicta, J. M. (2021, July). Penetration Test on Home Network Environments: A Cybersecurity Case Study. In 2021

[27] Setiawan, E. B., & Setiyadi, A. (2018, August). Web vulnerability analysis and implementation. In IOP conference series: materials science and engineering (Vol. 407, No. 1, p. 012081). IOP Publishing.

[28] Sheldon, F. T., Weber, J. M., Yoo, S. M., & Pan, W. D. (2012). The insecurity of wireless networks. IEEE Security & Privacy, 10(4), 54-61.

[29] Elhamahmy, M. E., & Sobh, T. S. (2011, May). Preventing Information Leakage Caused by Wardriving Attacks in Wi-Fi Networks. In the Global Conference on Aerospace Sciences and Aviation Technology (Vol. 14, No. AEROSPACE SCIENCES & AVIATION TECHNOLOGY, ASAT14–May 24-26, 2011, pp. 1-9). The Military Technical College.

[30] Nunez, J., Tran, V., & Katangur, A. (2019). Protecting the unmanned aerial vehicle from cyberattacks. In Proceedings of the Global Conference on Security and Management (SAM) (pp. 154- 157). The Steering Committee of The International Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[31] Kashyap, K., Noor, A., Saraswat, R., & Sharma, V. K. Learning of Penetration tool testing techniques Using Open Source Tools for Beginners

[32] van Rensburg, J. J., & Irwin, B. Wireless Security Tools. Computer Science, 83(944), 3924.

[33] Ortiz G& Keiny J. (2012), An Overview to BackTrack Penetrations Tools. Computer Engineering

[34] Ömer Aslan, Refik Samet, “Mitigating Cyber Security Attacks by Being Aware of Vulnerabilities and Bugs” September 2017, DOI: 10.1109/CW.2017.22 Conference: 2017 International Conference on Cyberworlds (CW)

[35] Ömer Aslan, Computer System and Third-Parties Vulnerabilities Increases the Risk of Cyberattacks January 2022, Conference: 7. International Congress of Academic Research At: Turkey

[36] Azaz Ahamed, Nafiz Sadman, “Automated Testing: Testing Top 10 OWASP Vulnerabilities of Government Web Applications in Bangladesh”June 2022,Conference: The Seventeenth International Conference on Software Engineering Advances ICSEA 2022, At: Lisbon, Portugal

[37] Ömer Aslan,"A Methodology to Detect Distributed Denial of Service Attacks",April 2022, Bilişim Teknolojileri Dergisi 15(2):149-158,DOI:10.17671/gazibtd.1002178

[38] Bitlis Eren, Üniversitesi Fen, “Ransomware Detection in Cyber Security Domain”July 2022,Bitlis Eren University Journal of Science and Technology 11(2):509-519 DOI: 10.17798/bitlisfen.1038966

[39] Ömer Aslan,Abdullah Asım Yılmaz, “A New Malware Classification Framework Based on Deep Learning Algorithms”, VOLUME 9, 2021

[40] Ömer Aslan, MERVE OZKAN-OKAY, “Intelligent Behavior- Based Malware Detection System onCloud Computing Environment”, June 2021 IEEE Access PP (99):1-1.