Towards Countering the Insider Reconnaissance Using a Combination of Shuffling and Diversity Moving Target Defense Techniques

Muhammad Faraz Hyder
Department of Software Engineering
NED University of Engineering & Technology
Karachi, Pakistan
farazh@neduet.edu.pk

Waseemullah
Department of Computer Science and IT
NED University of Engineering & Technology
Karachi, Pakistan
waseemu@neduet.edu.pk

Muhammad Umer Farooq
Department of Computer Science and IT
NED University of Engineering & Technology
Karachi, Pakistan
umer@neduet.edu.pk

Abstract-Moving Target Defense (MTD) has recently emerged as a significant cybersecurity technique. Software-Defined Networking (SDN) has the capability to design efficient network architecture due to its programmability and centralized control management. In this paper, a mechanism for the protection against insider reconnaissance has been proposed using a combination of diversity and a shuffling-based approach of MTD. In order to implement the shuffling technique, IP shuffling is used in the insider network. The IP addresses of internal hosts are mapped via real to virtual IP mapping through random IP generation from a pseudo-random mechanism. For the diversity, a multiple servers' platform is incorporated for different critical LAN services like Domain Name System (DNS), internal web services, etc. This combined diversity and shuffling approach significantly counters the insider reconnaissance targeting critical LAN services. The proposed scheme also exploited open-source IDS to block insider reconnaissance. The proposed solution was implemented using ONOS SDN controller, Mininet simulator, Snort IDS systems. The experimental results substantiate effective protection against insider network reconnaissance at a low computational cost.

Keywords-diversity; IP shuffling; insider reconiccance moving target defense; software defined networking; virtual IP

I. INTRODUCTION

Threats emerging from malicious insiders that have quite a clear picture of the internal resources are becoming more and more common [1]. Network reconnaissance is the initial stage of the cyber kill chain [2]. The notion is to collect information about the system and its attributes. Many different solutions have been proposed for the protection against these types of attack [3]. However, the existing work for protection against the network reconnaissance is mainly focused on the external attackers and subsequently the reconnaissance traffic generated from outsiders. Moving target is a cyber defense technique with the goal of constantly changing the attack surface in order to incommode the attacker to exploit the system [4-6]. This active cybersecurity has already drawn the attention of the research community in different domains including the security of cyber-physical systems [7, 8], network security [4], cloud security [9], IoT security [10], etc. Software-Defined Networking (SDN) [11] augments the MTD-based solution development due to its centralized network control, visibility, and separation of control and data planes. Therefore, several MTD solutions are based on SDN [5, 12, 13].

In this paper, a mechanism for protecting the critical DNS and Web Servers from reconnaissance attacks generating from inside the network has been developed. The notion of the work is the exploitation of the MTD mechanism for the protection of resources from insider reconnaissance. Moreover, we have adopted a combination of two different MTD techniques, i.e. Diversity and Shuffling. The work provides a three-layer protection against insider reconnaissance. In the first line of defense, the IP addresses of the nodes are periodically mapped to virtual IP addresses. These addresses are generated using pseudo-random number generators in order to enhance the randomness. The mechanism provides the functionality of all internal communication happening via a virtual IP address. The second line of defense is the platform-level diversity of DNS and Web Services. The third protection mechanism is the use of IDS to detect and block malicious insiders generating reconnaissance traffic. These three approaches substantially counter the internal reconnaissance while ensuring that the information gained by the insider during the reconnaissance is not correct as it changes after a specific period.

The fundamental motivation behind the MTD based system is to increase the uncertainty and confusion regarding the

Corresponding author: Muhammad Faraz Hyder

information collected by attackers through constantly changing the attack surface [14]. It is an active cybersecurity technique with the objective of making cybersecurity an equal playing field for both the attacker and the defender. There are three broad categories of MTD, namely diversity, redundancy, and shuffling [15]. The diversity technique provides different platforms, software, programming languages, and networks. In the case of shuffling techniques, different system parameters are shuffled either periodically or on the basis of certain events. In redundancy, replicas of the resources are created. These replicated and redundant resources substantially increase the uncertainty for the attacker. Most of the work in the domain of MTD exploits one of the basic three approaches. However, a combination of these approaches has not been exploited in detail. The amalgamations of these techniques will enhance the performance of the MTD solution and increase attacker uncertainty. SDN is getting popular in designing security solutions [16]. The centralized controlling attributes enable greater ease for designing the MTD solution. It's also popular to design MTD for network security [17, 18], cyber-physical systems [7], ad hoc networks [19, 20], cloud security [9, 19], etc.

Insider attacks are gaining momentum [1, 20]. There is an initial level of work for the protection of the first stage of the cyber kill chain, i.e. reconnaissance [21]. Authors in [22] proposed a scheme to counter external reconnaissance using SDN-based virtual topologies. In [23], the authors suggested a bio-inspired technique to mitigate insider reconnaissance attacks. Insider threat detection based upon a reality game-based approach was proposed in [24].

II. THE PROPOSED SCHEME

The proposed scheme has three levels of defense. The first one is the IP shuffling approach for different nodes and servers. The second one is based upon the diversity of platforms for Web and DNS servers. The third level of defense is the detection of insider reconnaissance via open-source IDS solution and subsequently blocking the malicious hosts generating such traffic. The high-level diagram is depicted in Figure 1.

The MTD is created using the ONOS SDN controller that consists of multiple switches and different hosts connected. Figure 2 depicts the communication between two hosts. It also presents the network flow between these hosts. The communication inside the network is happening via virtual IP addresses that are constantly changing. When a host initiates the traffic to other hosts in the network, then communication is mapped to their corresponding virtual IPs. There are several steps involved in this communication. The application running in the controller will modify the IP address of the host to convert it into a virtual IP address. The frequency for IP shuffling is set to be 30 seconds for attaining a time-based MTD mechanism. The SDN controller injects the necessary flows based upon the new IP addresses for smooth communication inside the network.

The second line of defense counters insider reconnaissance targeting specific services like DNS and Web servers. To protect against this type of attack, multiple platforms are used. In the case of DNS, the server was prepared using Bind9 and Unbound DNS. Similarly, there are different platforms for web servers, like Apache, Nginx, and IIS. Within these platforms, different versions are also used to increase the uncertainty for the attackers. When the insider performs reconnaissance to gather information about the DNS or the Web servers, then they will get diversified platform information.

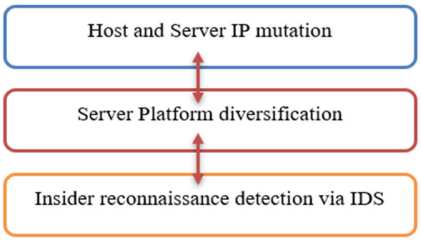

Fig. 1. The multi-layered defense approach against insider reconnaissance attacks.

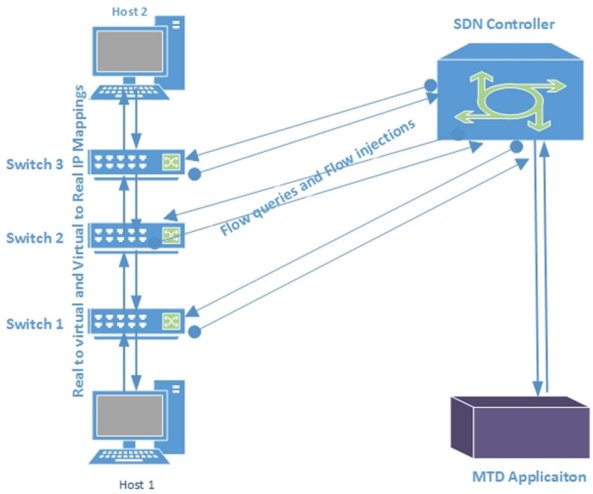

Fig. 2. Traffic flow sequence during IP mapping from real to virtual and vice versa.

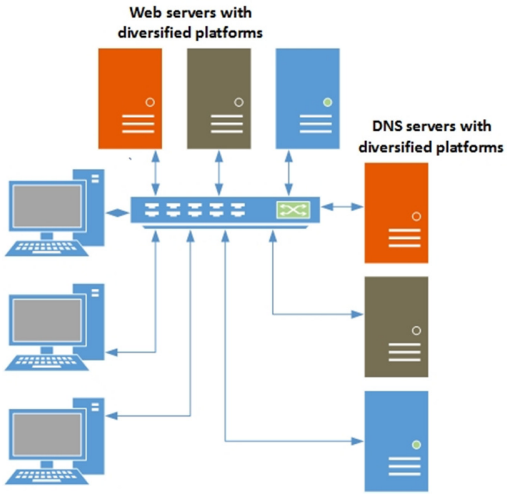

Fig. 3. Server platform diversification.

The proposed solution also utilized the open-source IDS Snort to detect and block the insider generating the reconnaissance traffic. This is the third line of defense against insider threats. Figure 3 depicts the server platform diversification for DNS and Web Servers. The attacker performing scanning will get different results of specific web and DNS platforms. Figure 4 represents the Snort platform analyzing the traffic for detection of reconnaissance traffic. The graphical interface of the Snort platform is depicted in Figure 5.

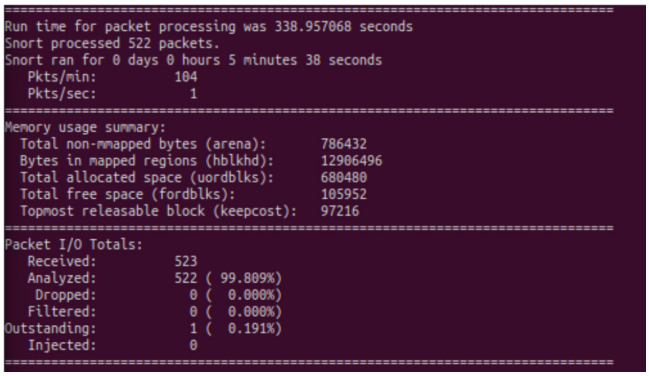

Fig. 4. Snort IDS platform analyzing packets.

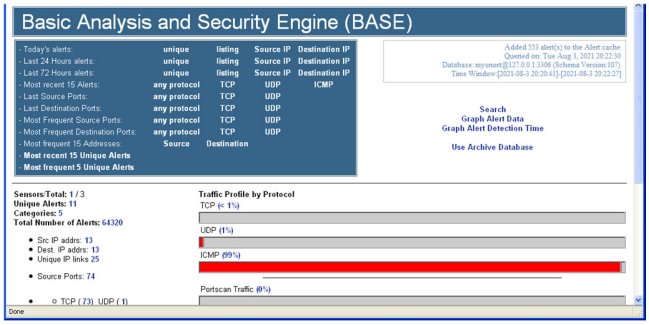

Fig. 5. Graphical interface of the Snort IDS platform.

III. EXPERIMENTAL SETUP

We used ONOS SDN Controller [25], Mininet simulator [26], and Snort IDS [27]. Regarding the server machines, we used different platforms for webserver implementation including Apache [28], Nginx [29], and IIS [30], while DNS implementation BIND9 [31], Unbound DNS [32], and PowerDNS [33] packages were selected. On the SDN network, class A IP addresses were assigned. sFlow [34] was used for collecting different statistical parameters of the network. The experimental setup was implemented on a Dell server having 32GB RAM. To generate the reconnaissance traffic, we have used Nmap [35]. The experimental topology is depicted in Figure 6. The attacker first generates the reconnaissance traffic against the other internal hosts. However, all internal transmission is based upon the mapping from real to virtual IP addresses mapping. This mapping also uses pseudo-random number generators to produce virtual IPs. The information gained by the attacker in one iteration gets invalidated due to virtual IP randomization. In the second phase, the attacker targets the DNS and Web servers' platforms.

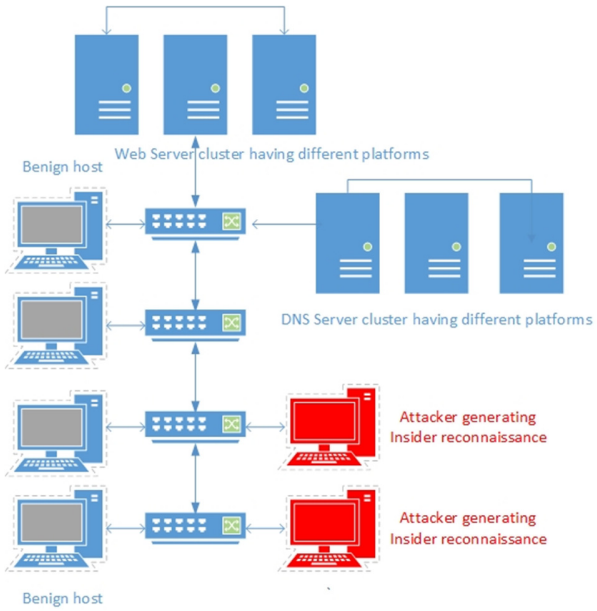

Fig. 6. The experimental topology.

IV. RESULTS AND DISCUSSION

We assumed that the attacker can perform a maximum of 10 scan probes at a time. Table I represents the IP addresses on the network as observed by the attacker in different iterations. The attackers perform multiple reconnaissance attacks. The attackers observed different IP schemes and addresses due to the IP randomization through the proposed MTD scheme. This substantially increases the confusion for the attackers, because the knowledge gained in each iteration becomes void in the next. Figure 7 illustrates the IP shuffling results for different iterations. The attackers discovered different number of IP addresses in different iterations. However, in different iterations attackers may correctly identify the previous IP addresses. The percentage of getting the same IP addresses in consecutive iterations is below 5%. We considered the generic case of i^{th} and i^{th+1} iterations.

TABLE I. IP ADDRESSES DISCOVERED IN DIFFERENT ITERATIONS OF RECONNAISSANCE BY THE INSIDER ATTACKER

IP addresses discovered in:			
1st iteration	**2nd iteration**	**3nd iteration**	**4rth iteration**
192.168.10.4	10.5.7.9	172.16.12.5	10.6.7.3
192.168.10.5	10.5.7.10	172.16.12.6	10.6.7.4
192.168.10.6	10.5.7.11	172.16.12.7	10.6.7.5
192.168.10.7	10.5.7.12	172.16.12.8	10.6.7.6
192.168.10.8	10.5.7.13	172.16.12.9	10.6.7.7
192.168.10.9	10.5.7.14	172.16.12.10	10.6.7.8
192.168.10.10	10.5.7.15	172.16.12.11	10.6.7.9
192.168.10.11	10.5.7.16	172.16.12.12	10.6.7.10
192.168.10.12	10.5.7.17	172.16.12.13	10.6.7.11
192.168.10.13	10.5.7.18	172.16.12.14	10.6.7.12

Table II depicts the diversified DNS and Web servers' platform observed by the attackers while running probing traffic against these servers. Since our scheme deploys diversified platforms, the attackers observe multiple platforms. This substantially increased the attacker confusion.

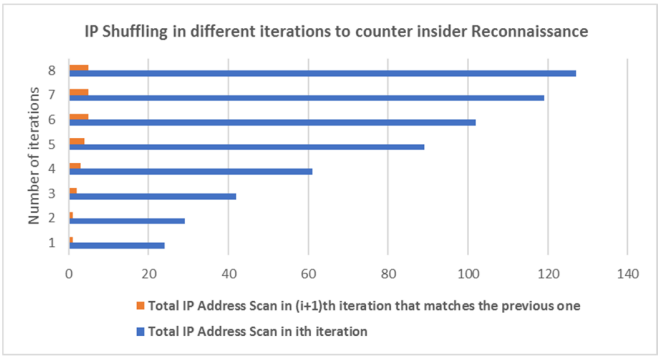

Fig. 7. IP Shuffling to counter insider reconnaissance.

Table III indicates the IP addresses of the malicious insiders generating reconnaissance traffic being blocked by the third line of defense of our scheme i.e., the IDS Snort. The first column in Table III is the number of distinct attackers, the second column indicates the maximum number of probes generated by the attacker. The third column is the multiple of the first two, i.e. the total generated probes. The IDS is able to detect and blocked on average approximately 85% of malicious attackers. Overall, the proposed scheme successfully counters the insider reconnaissance using the three-level defense level MTD technique.

TABLE II. PLATFORM DIVERSITY FOR WEB AND DNS SERVICES

Web server IP addresses	Web server platform detected	DNS server IP addresses	DNS server platform detected
192.168.10.10	Apache 2.4.48	192.168.10.13	Bind 9.12
10.5.7.15		10.5.7.18	
172.16.12.11	nginx-1.21.1.	172.16.12.14	Unbound 1.13.2
10.6.7.9	IIS 10.0 Express	10.6.7.12	PowerDNS 4.5.1

TABLE III. ATTACKER IP ADDRESSES BLOCKED BY IDS

No. of malicious IP addresses generating scans	No. of scans generated by an individual attacker	Total No. of insider reconnaissance attempts	Malicious IP addresses detected and blocked by the IDS	Malicious IP addresses detected and blocked by the IDS (%)
N	**M**	**T=N×M**	**B**	**%**
10	10	100	8	80%
20	10	200	17	85%
30	10	300	26	87%
40	10	400	35	88%
50	10	500	42	84%
60	10	600	53	88%
70	10	700	60	86%
80	10	800	69	86%
90	10	900	76	84%
100	10	1000	86	86%

V. COMPARISON OF THE PROPOSED SCHEME WITH STATE-OF-THE-ART TECHNIQUES

Table IV summarizes the comparison of the proposed scheme with the state-of-the-art existing solutions. The first advantage of our scheme is the exploitation of MTD for insider reconnaissance protection. The existing work in the literature [22-24] focuses on the protection of external reconnaissance. The second advantage of our technique is the combination of MTD techniques for insider reconnaissance protection. Moreover, our scheme is based upon SDN which provides greater flexibility in designing MTD solutions. Only the work presented in [22] exploited SDN-based MTD for probing traffic protection. However, their work focused on external reconnaissance protection only. Hence our proposed SDN-based combination of MTD technique is quite an efficient one.

TABLE IV. COMPARISON OF THE PROPOSED IMPLEMENTATION WITH EXISTING SOLUTIONS

	Insider reconnaissance protection	Multiple MTD techniques	SDN-based MTD solution
Proposed	✓	✓	✓
[22]	×	×	✓
[23]	×	×	×
[24]	×	×	×

VI. CONCLUSION AND FUTURE WORK

In this paper, a protection mechanism against insider reconnaissance traffic has been developed by combining the Randomization and Diversification MTD approaches inside an SDN-based network along with IDS-based detection. The work elaborated the effectiveness of the scheme for two important services, i.e. DNS and Web. The proposed scheme provides three levels of defense: IP randomization and platform diversity for DNS and Web Servers and IDS-based detection and blockage. The developed solution effectively throttles the insider probing traffic with minimal computational cost.

In the future, we will extend our technique for privacy enhancement for critical services. An adversary while observing the DNS traffic can cause privacy disclosure by identifying the URLs visited by the users. The proposed approach can be extended to protect against such attacks.

REFERENCES

[1] L. Liu, O. De Vel, Q.-L. Han, J. Zhang, and Y. Xiang, "Detecting and Preventing Cyber Insider Threats: A Survey," *IEEE Communications Surveys Tutorials*, vol. 20, no. 2, pp. 1397–1417, 2018, https://doi.org/10.1109/COMST.2018.2800740.

[2] T. Yadav and A. M. Rao, "Technical Aspects of Cyber Kill Chain," in *International Symposium on Security in Computing and Communication*, Kochi, India, Aug. 2015, pp. 438–452, https://doi.org/10.1007/978-3-319-22915-7_40.

[3] M. I. Al-Saleh, Z. A. Al-Sharif, and L. Alawneh, "Network Reconnaissance Investigation: A Memory Forensics Approach," in *10th International Conference on Information and Communication Systems*, Irbid, Jordan, Jun. 2019, pp. 36–40, https://doi.org/10.1109/IACS.2019.8809084.

[4] S. Sengupta, A. Chowdhary, A. Sabur, A. Alshamrani, D. Huang, and S. Kambhampati, "A Survey of Moving Target Defenses for Network Security," *IEEE Communications Surveys Tutorials*, vol. 22, no. 3, pp. 1909–1941, 2020, https://doi.org/10.1109/COMST.2020.2982955.

[5] M. F. Hyder and M. A. Ismail, "INMTD: Intent-based Moving Target Defense Framework using Software Defined Networks," *Engineering, Technology & Applied Science Research*, vol. 10, no. 1, pp. 5142–5147, Feb. 2020, https://doi.org/10.48084/etasr.3266.

[6] M. H. H. Khairi, S. H. S. Ariffin, N. M. A. Latiff, A. S. Abdullah, and M. K. Hassan, "A Review of Anomaly Detection Techniques and Distributed Denial of Service (DDoS) on Software Defined Network (SDN)," *Engineering, Technology & Applied Science Research*, vol. 8, no. 2, pp. 2724–2730, Apr. 2018, https://doi.org/10.48084/etasr.1840.

[7] B. Potteiger, Z. Zhang, and X. Koutsoukos, "Integrated moving target defense and control reconfiguration for securing Cyber-Physical systems," *Microprocessors and Microsystems*, vol. 73, Mar. 2020, Art. no. 102954, https://doi.org/10.1016/j.micpro.2019.102954.

[8] M. Higgins, K. Mayes, and F. Teng, "Enhanced Cyber-Physical Security Using Attack-resistant Cyber Nodes and Event-triggered Moving Target Defence," *arXiv:2010.14173 [cs, eess]*, Oct. 2020, Accessed: Oct. 03, 2021. [Online]. Available: http://arxiv.org/abs/2010.14173.

[9] M. Torquato and M. Vieira, "Moving target defense in cloud computing: A systematic mapping study," *Computers & Security*, vol. 92, May 2020, Art. no. 101742, https://doi.org/10.1016/j.cose.2020.101742.

[10] R. E. Navas, F. Cuppens, N. Boulahia Cuppens, L. Toutain, and G. Z. Papadopoulos, "MTD, Where Art Thou? A Systematic Review of Moving Target Defense Techniques for IoT," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 7818–7832, May 2021, https://doi.org/10.1109/JIOT.2020.3040358.

[11] Y. Djeldjeli and M. Zoubir, "CP-SDN: A New Approach for the Control Operation of 5G Mobile Networks to Improve QoS," *Engineering, Technology & Applied Science Research*, vol. 11, no. 2, pp. 6857–6863, Apr. 2021, https://doi.org/10.48084/etasr.4016.

[12] S. Debroy *et al.*, "Frequency-Minimal Utility-Maximal Moving Target Defense Against DDoS in SDN-Based Systems," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 890–903, Jun. 2020, https://doi.org/10.1109/TNSM.2020.2978425.

[13] D. P. Sharma *et al.*, "Dynamic Security Metrics for Software-Defined Network-based Moving Target Defense," *Journal of Network and Computer Applications*, vol. 170, Nov. 2020, Art. no. 102805, https://doi.org/10.1016/j.jnca.2020.102805.

[14] R. Zhuang, S. A. DeLoach, and X. Ou, "Towards a Theory of Moving Target Defense," in *First ACM Workshop on Moving Target Defense*, Scottsdale, AR, USA, Nov. 2014, pp. 31–40, https://doi.org/10.1145/2663474.2663479.

[15] J.-H. Cho *et al.*, "Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense," *IEEE Communications Surveys Tutorials*, vol. 22, no. 1, pp. 709–745, 2020, https://doi.org/10.1109/COMST.2019.2963791.

[16] O. Yurekten and M. Demirci, "SDN-based cyber defense: A survey," *Future Generation Computer Systems*, vol. 115, pp. 126–149, Feb. 2021, https://doi.org/10.1016/j.future.2020.09.006.

[17] A. Chowdhary, A. Alshamrani, D. Huang, and H. Liang, "MTD Analysis and evaluation framework in Software Defined Network (MASON)," in *ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*, New York, NY, USA, Mar. 2018, pp. 43–48, https://doi.org/10.1145/3180465.3180473.

[18] A. Chowdhary, S. Pisharody, and D. Huang, "SDN based Scalable MTD solution in Cloud Network," in *ACM Workshop on Moving Target Defense*, Vienna, Austria, Oct. 2016, pp. 27–36, https://doi.org/10.1145/2995272.2995274.

[19] H. Alavizadeh, J. Jang-Jaccard, and D. S. Kim, "Evaluation for Combination of Shuffle and Diversity on Moving Target Defense Strategy for Cloud Computing," in *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, USA, Aug. 2018, pp. 573–578, https://doi.org/10.1109/TrustCom/BigDataSE.2018.00087.

[20] D. C. Le and N. Zincir-Heywood, "Anomaly Detection for Insider Threats Using Unsupervised Ensembles," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1152–1164, Jun. 2021, https://doi.org/10.1109/TNSM.2021.3071928.

[21] K. Park, S. Woo, D. Moon, and H. Choi, "Secure Cyber Deception Architecture and Decoy Injection to Mitigate the Insider Threat," *Symmetry*, vol. 10, no. 1, Jan. 2018, Art. no. 14, https://doi.org/10.3390/sym10010014.

[22] S. Achleitner, T. F. La Porta, P. McDaniel, S. Sugrim, S. V. Krishnamurthy, and R. Chadha, "Deceiving Network Reconnaissance Using SDN-Based Virtual Topologies," *IEEE Transactions on Network and Service Management*, vol. 14, no. 4, pp. 1098–1112, Dec. 2017, https://doi.org/10.1109/TNSM.2017.2724239.

[23] A. Nicolaou, S. Shiaeles, and N. Savage, "Mitigating Insider Threats Using Bio-Inspired Models," *Applied Sciences*, vol. 10, no. 15, Jan. 2020, Art. no. 5046, https://doi.org/10.3390/app10155046.

[24] S. Wasko *et al.*, "Using alternate reality games to find a needle in a haystack: An approach for testing insider threat detection methods," *Computers & Security*, vol. 107, Aug. 2021, Art. no. 102314, https://doi.org/10.1016/j.cose.2021.102314.

[25] P. Berde *et al.*, "ONOS: towards an open, distributed SDN OS," in *3rd workshop on Hot topics in software defined networking*, Chicago, IL, USA, Aug. 2014, pp. 1–6, https://doi.org/10.1145/2620728.2620744.

[26] R. L. S. de Oliveira, C. M. Schweitzer, A. A. Shinoda, and L. R. Prete, "Using Mininet for emulation and prototyping Software-Defined Networks," in *IEEE Colombian Conference on Communications and Computing*, Bogota, Colombia, Jun. 2014, pp. 1–6, https://doi.org/10.1109/ColComCon.2014.6860404.

[27] M. Roesch, "Snort – Lightweight Intrusion Detection for Networks," in *Lisa*, Washington, DC, USA, Nov. 1999, pp. 229–238.

[28] R. R. Zebari, S. R. M. Zeebaree, and K. Jacksi, "Impact Analysis of HTTP and SYN Flood DDoS Attacks on Apache 2 and IIS 10.0 Web Servers," in *International Conference on Advanced Science and Engineering*, Duhok, Iraq, Oct. 2018, pp. 156–161, https://doi.org/10.1109/ICOASE.2018.8548783.

[29] C. Nedelcu, *Nginx HTTP Server*, Second edition. Birmingham, UK: Packt Publishing, 2013.

[30] Y. Yan, P. Guo, B. Cheng, and Z. Zheng, "An experimental case study on the relationship between workload and resource consumption in a commercial web server," *Journal of Computational Science*, vol. 25, pp. 183–192, Mar. 2018, https://doi.org/10.1016/j.jocs.2017.05.019.

[31] T. Jinmei and P. Vixie, "Implementation and evaluation of moderate parallelism in the BIND9 DNS server," in *USENIX Annual Technical Conference*, Berkeley, CA, United States, Jun. 2006, pp. 115–128.

[32] S. Son and V. Shmatikov, "The Hitchhiker's Guide to DNS Cache Poisoning," in *International Conference on Security and Privacy in Communication Systems*, Singapore, Singapore, Sep. 2010, pp. 466–483, https://doi.org/10.1007/978-3-642-16161-2_27.

[33] G. Lencse and S. Repas, "Performance analysis and comparison of four DNS64 implementations under different free operating systems," *Telecommunication Systems*, vol. 63, no. 4, pp. 557–577, Dec. 2016, https://doi.org/10.1007/s11235-016-0142-x.

[34] K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras, and V. Maglaris, "Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments," *Computer Networks*, vol. 62, pp. 122–136, Apr. 2014, https://doi.org/10.1016/j.bjp.2013.10.014.

[35] G. F. Lyon, *Nmap network scanning: Official Nmap project guide to network discovery and security scanning*. Sunnyvale, CA, USA: Insecure. Com LLC, 2008.