# An Analysis of Switchport Vulnerabilities and MTD Techniques Applied to Mitigate the Port Scanning Threats

R.G.C. Upeksha
*Faculty of Computing and IT,*
*Sri Lanka Technology Campus (SLTC)*
upeksha.r@sltc.ac.lk

R.G.N. Meegama
*Department of Computer Science, Faculty of Applied Sciences,*
*University of Sri Jayewardenepura, Sri Lanka*
rgn@sjp.ac.lk

***Abstract*** **Moving Target Defense (MTD) techniques are increasingly employed to enhance network security. MTD aims to disrupt the static nature of networks, which can facilitate attackers by easily extracting crucial network information for future vulnerability exploitation. This study investigates the potential synergy between MTD and switchport vulnerabilities. Furthermore, this paper presents a comprehensive study on Moving Target Defense and network scanning, a well-known reconnaissance technique typically involving three main phases: host detection, port discovery, and vulnerability assessment. The analysis reveals two key findings: First, the limited scope of existing MTD solutions applied to mitigate different network threats and attacks. Second, the study identifies vulnerabilities in network switches and proposed potential mitigation strategies. The systematic review analyzed twelve recent publications on MTD applications and five on switch vulnerability solutions. Moreover, the literature review suggests a promising area for further research: exploring the application of MTD techniques to mitigate the threats posed by port scanning.**

***Keywords- moving target defense, network security, port scanning, switchport attacks***

## I. INTRODUCTION

Humans exhibit diverse behavioral patterns stemming from their intelligence and thinking abilities. From a young age, people engage in various investigative actions, especially as they adapt to their environment. Driven by a natural desire for safety and security, humans inherently tend to observe and investigate their surroundings. This innate human behavior, which can be characterized as reconnaissance, has evolved over time. People have found reconnaissance to be a valuable tool in various endeavors, including hunting, stalking, gathering, warfare, and numerous other situations [1]. With malicious intent, individuals often attempt to identify vulnerabilities and weaknesses in their targets by employing various techniques, such as espionage and communication interception, etc. [2]. While not the attack itself, this action serves as a critical and proactive step, significantly increasing the likelihood of its success.

Modern attackers leverage the same concept to gather information about computer and network systems. Exploiting discovered weaknesses, vulnerabilities, and critical network details, they can launch targeted attacks. Network reconnaissance, the initial stage of such attacks, aims to collect valuable information within a target network, such as the number of active nodes and software versions [3]. This reconnaissance can be categorized as either active, involving direct connections to the target, or passive, relying on indirect methods like external data sources [4]. Both approaches utilize various reconnaissance techniques such as Scanning, Fingerprinting, Enumeration, Traffic Sniffing and Honeypot Detection [5]. Network scanning, a vital reconnaissance technique employed by both defenders and attackers, consists of three main phases: host detection, port discovery, and vulnerability assessment.

Host Detection During the first phase of network scanning, attackers employ various techniques like ICMP echo requests to identify active hosts within networks. This phase reveals operational hosts and their IP addresses and gathers additional information like live status. Additionally, network sniffing tools like tcpdump and Wireshark can be used to passively collect network data, primarily affecting the data link and IP layers.

Port Scanning Having identified active hosts within the network, attackers leverage advanced port scanning techniques to glean critical network information such as port status, running services, software versions, and operating systems. One such advanced technique involves spoofing, which allows attackers to perform port scans by masking their true IP address with a trusted one [6].

ARP spoofing ranks among the critical network attacks. The Address Resolution Protocol (ARP), a data link layer protocol, establishes communication between devices by mapping IP addresses to their corresponding physical (MAC) addresses. To achieve this, a sender broadcasts an ARP request containing the target device's IP address. If the target device recognizes its IP address, it responds with its MAC address, enabling communication to proceed. Attackers exploit this process in ARP spoofing by sending forged ARP replies with their own MAC address, tricking other devices into directing traffic to them instead of the intended recipient. The vulnerability lies in the broadcast nature of ARP requests. Attackers can exploit this by sending deceptive ARP replies containing a forged (IP, MAC) address before the intended recipient responds. This "poisons" the ARP cache of other devices, tricking them into directing traffic to the attacker instead of the legitimate host. This opens the network to various attacks like Man-in-the-Middle (MitM), Denial-of-Service (DoS), and host impersonation., etc [7].

Modern attackers increasingly rely on slow port scanning, a challenging reconnaissance technique capable of evading even established Intrusion Detection Systems (IDS) [8]. Unlike conventional scans, slow scans employ tactics designed to bypass detection: randomizing significant time intervals between probes and exploiting

diverse scan sources. The protracted nature of these scans introduces an element of uncertainty, further complicating their identification by IDS. [9]. To identify vulnerabilities in endpoints, attackers often leverage protocol-based port scans. These scans utilize various protocols like TCP, UDP, SCTP, ICMP, and FTP to probe for open ports and potential weaknesses.

### *A. Moving Target Defense(MTD)*

The widespread use of interconnected devices in organizations has led to the rise of complex, automated network systems that facilitate communication and information sharing. However, a major concern in network security lies in the defensive and offensive asymmetry [10]. This concept describes the imbalance between the technologies and strategies employed by attackers to compromise systems and defenders to safeguard them [11]. Several factors contribute to this asymmetry such as certainty of network configurations where attackers can often readily analyze a network's configuration, gaining valuable insights into its vulnerabilities, static nature of network structure where network structures tend to be relatively static, making it easier for attackers to develop targeted exploit and consistency of network elements which is the use of standardized protocols and components in networks can create predictable patterns that attackers can leverage.

Moving Target Defense (MTD) aims to address the information asymmetry caused by the static nature of network systems by introducing uncertainty into computer and network systems. This approach seeks to level the playing field between attackers and defenders [10].

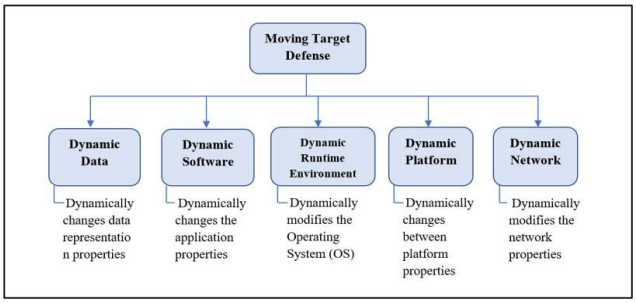



Fig. 1 Classification of MTD Techniques: The five core MTD categories (Dynamic Data, Software, Runtime Environment, Platform, and Network), illustrating the defensive layers available to introduce uncertainty and disrupt the Cyber Kill Chain.

The concept of MTD draws inspiration from various real-world applications of "moving targets," including Chameleons' camouflage in the wild: Similar to how chameleons blend into their surroundings, MTD aims to make systems dynamically change their configurations, reducing the attacker's ability to exploit vulnerabilities.

Moving targets in weapon shooting: Just as moving targets are more difficult to hit, MTD makes systems less predictable, increasing the attacker's difficulty in launching successful attacks.

Adaptability of cryptography: Cryptographic algorithms are constantly evolving to stay ahead of attackers, reflecting the core principle of MTD, which emphasizes continuous change to enhance security.

The Cyber Kill Chain framework outlines the typical stages of a cyberattack, consisting of seven phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives [12]. Moving Target Defense (MTD) techniques, categorized into five main levels (Fig. 1), can be strategically applied to disrupt these attack phases. Specifically, dynamic network techniques, which continuously change network attributes like IP addresses and ports, can hinder the attacker's reconnaissance phase. By preventing attackers from effectively gathering essential network information about the target, these techniques disrupt their ability to progress through the Cyber Kill Chain [13].

## II. LITERATURE REVIEW

### *A. Moving Target Defense: Principles, Classifications, and Existing Applications*

Moving Target Defense (MTD) has been deployed in various fields to combat fraudulent observations. In computing contexts, diverse MTD strategies safeguard against security threats. Extensive research has explored the use of MTD to develop network security solutions and establish trust within network environments. Several research studies have discussed the application of Moving Target Defense (MTD) in cyber-physical systems, where sensors are often used for multiple purposes. MTD employs a proactive mechanism that dynamically and continuously changes system parameters through a switching structure. This approach can mitigate both sensor and actuator attacks [14], Furthermore, switching supervisory control between sensors can mitigate sensor deception attacks on event-driven systems [15]. Additionally, research has been conducted on mitigating stealthy sensor attacks by combining the Nash equilibrium strategy with a Moving Target Defense (MTD) strategy based on detector entry switching [16].

Moreover, Moving Target Defense (MTD) techniques, specifically those focusing on dynamic network configurations, address the reconnaissance phase of the cyber kill chain. By dynamically altering network configurations, they hinder efforts to discover and scan targets. One of the most widely used approaches in dynamic network MTD techniques is IP address randomization. MUTE [17] is an architecture that dynamically changes IP addresses and routes within a network. This approach disrupts attackers' ability to perform reconnaissance, launch DoS attacks, and establish botnets. The derived technique, known as Random Host Mutation (RHM), is a key component of MUTE and [18], [19] by the same author of MUTE, which makes the end-point unidentifiable by assigning virtual IP addresses that change randomly in a synchronized manner. Both the research has considered preserving the integrity, manageability, and performance of the network system.

In addition, another solution that uses IP randomization has been proposed against DDoS attacks, which is named FastMove [20], which uses DNS facilities to hide the server addresses from the attackers. In IP address randomization some researchers suggest refreshing and reassigning IP addresses between real and decoy nodes can lead to service disruptions in TCP/IP services. To avoid that type of disruption, an effective approach has been proposed, which introduces an optimal randomization policy [21].

Software-Defined Networking (SDN) is a trending technology where it is possible to communicate with the hardware infrastructure of the network, using the provided software-based controllers and application programming

interfaces (APIs). Most of the recent research studies on MTD are based on software-defined networks. A new mechanism has been proposed to mitigate an emerging type of DDoS attack called Crossfire using Floodlight SDN Controller and Mininet Emulator. Moreover, this mechanism performs route randomization which can reduce the link flooding [22].

An emerging version of another DDoS attack named Blind DDoS attacks targets the special structure of the SDNs' and the controller in SDN is found to be much more vulnerable to failures. To mitigate these attacks an MTD system is proposed which maintains a multiple-controller pool that changes the controller dynamically as the moving target [23].

OpenFlow is one of the first Software-Defined Networking (SDN) standards and it has been used to implement the MTD mechanisms. OpenFlow Random Host Mutation is one such technique proposed, which can randomly assign virtual IP addresses to cover the real ones [24] and there are similar studies that have used OpenFlow to establish MTD techniques like IP shuffling and host mutating [25], [26].

Potential future applications for MTD include dynamic switchport behavior modification, such as randomized MAC-to-port mapping and dynamic VLAN reallocation. These techniques could significantly disrupt the reconnaissance phase by rapidly changing the target profile of a switchport, specifically countering port scanning threats.

### *B. Network Reconnaissance and Advanced Port Scanning Techniques*

A significant body of research has proposed solutions to defend against network reconnaissance activities, utilizing various approaches beyond Moving Target Defense (MTD). A recent study explored the use of Software Defined Networking (SDN) to defend against port scanning and Denial-of-Service (DoS) attacks. This study implemented two techniques: Credit-Based Threshold Random Walk (CB-TRW) and Rate Limiting (RL), to monitor for malicious activities and violations of network security policies [27].

A Markov model of an SDN switch has been proposed which captures the target flows [28] and an approach to detect slow port scanning has been introduced with sequential steps (i.e. data capturing, packet recognition, scanning filter, and detection filter) [21].

Cyber deception is another technique used to protect against network reconnaissance activities. This technique redirects traffic from the real network to an identical deception network (D-Net) [29]. While D-Nets are a common implementation, other deception topologies exist, including vulnerable host placement, honeypot placement, delay, and bandwidth adjustment, and more [30].

Recent studies specifically demonstrate the practical application of MTD techniques to disrupt the reconnaissance phase. This includes developing lossless MTD mechanisms focusing on IP address mutation in edge and core network switches to prevent the adversary from locating real nodes without impacting Quality of Service [31].

Furthermore, the temporal randomization of network attributes such as IP and MAC addresses and port numbers has been successfully utilized in real-time to proactively mitigate reconnaissance attacks, highlighting a direct MTD application against port scanning [32].

### *C. In-depth Analysis of Switchport Vulnerabilities and Traditional Mitigations*

Network switches play a crucial role in network communication. They connect various network devices to form a Local Area Network (LAN). Additionally, switches can function as distribution layer switches in higher network tiers. Several comprehensive studies have identified vulnerabilities and problems within network switches and proposed various solutions to address them.

Authors of [33] investigated solutions for compromised switches in Software Defined Networks (SDNs) using Service Function Chaining (SFC). SFC offers a flexible virtual chain of network services, but it can be vulnerable to compromised switches. These switches can be exploited by attackers to manipulate data packets without detection, such as dropping, forwarding, duplicating, or modifying them. The proposed solution modifies the network topology to isolate and remove the compromised switch while maintaining the functionality of the service chain.

The proposed solution in [34] is an intruder monitoring system that enhance the network security. The study highlights how ARP spoofing attacks can be used to observe, manipulate, and insert data into network traffic, detectable through network switches. The proposed solution involves leveraging VLANs (Virtual LANs) for logical network segmentation. While this approach offers a simple and straightforward method for network separation, it remains less secure and vulnerable compared to physically isolating devices.

A mutation-based fuzz testing approach specifically for protocols based on the Media Access Control (MAC) layer is proposed in [35]. The study demonstrates that this approach is effective in finding vulnerabilities compared to other fuzz testing methods. This is because mutation-based fuzz testing is an efficient technique for enhancing protocol security. The authors focused on two primary protocols on the MAC layer: File Transfer Protocol (FTP) and Port Negotiation Discovery Protocol (PN-DCP). The identified vulnerabilities include long strings before authentication, buffer overflows in the parameter fields "site chmod" and "REST" for FTP, and a format string vulnerability in PN-DCP.

Existing vulnerabilities in systems can be categorized into three main types, as identified in the research [36] : technology weaknesses, configuration weaknesses, and security policy weaknesses. The research further highlights that switches are susceptible to layer 3 attacks, which target the network layer of the Open Systems Interconnection (OSI) model. Examples of such layer 3 attacks include Denial-of-Service (DoS) attacks (e.g., ping floods, smurf attacks), VLAN hopping, spoofing attacks, and routing attacks. Private VLANs (PVLANs) introduce their own set of vulnerabilities, which can be exploited through various means. VLAN hopping attacks can exploit the isolation provided by PVLANs by constraining ports.

Additionally, misconfigurations and complex PVLAN configurations can be leveraged by attackers. MAC flooding attacks primarily target PVLAN configurations, while misconfigurations create their own set of vulnerabilities. The author proposes a comprehensive security strategy that incorporates various measures to address different network attacks, including those targeting

VLANs. This strategy focuses on implementing robust security policies at the switch port level. These policies include deactivating unused ports, utilizing dedicated VLAN Intrusion Detection Systems (IDS) for trunk ports to prevent VLAN hopping attacks, and applying port security measures such as sticky, static, and dynamic secure MAC addresses.

A research focusing on layer-two attacks targeting switches and routers which examined vulnerabilities related to VLAN hopping, private VLANs, the Spanning-Tree protocol, CAM table overflow, starvation attacks and MAC spoofing is proposed in[37]. As a solution, they propose implementing a server called an ”AAA Server,” which stands for Authentication, Authorization, and Accounting. This server would enhance network security by providing essential Authentication by verifying the identities of users and devices attempting to access the network, Authorization through determining the level of access granted to authenticated users and devices based on their permissions and Accounting by tracking and logging user and device activity on the network for auditing and security analysis purposes.

By employing an AAA server, network administrators can gain a centralized and comprehensive approach to managing network access and security. Moreover, Cisco Catalyst 6000 switch series and Cisco Catalyst 6500 and 6800 switch series are popular for long-standing, modular switch-class platforms and for high performance respectively. Still, it was reported that these switch series are having vulnerabilities that can be potentially exploited by attackers. These vulnerabilities include DoS vulnerability, 802.1x Authentication Bypass, OpenSSH Vulnerabilities, Crafted Layer 2 Frame Vulnerabilities etc. Crafted Layer 2 Frame Vulnerability involved how switches are handling crafted or malformed layer 2 frames and Cisco 6000/6500/7600 series are prone to exploitation through this vulnerability.

Attackers could create inconsistencies, triggering these vulnerabilities. This could involve manipulating fields related to MAC addresses or other layer 2 header information which can lead to MAC spoofing attacks. Furthermore, Cisco Catalyst 8500 Series Edge Platforms with higher-performance are having significant vulnerabilities including Cisco IOS XE Software Virtual Fragmentation Reassembly Denial of Service Vulnerability (CVE-2023-20027), Cisco IOS XE Software IOx Application Hosting Environment Privilege Escalation Vulnerability (CVE-2023-20065) etc. The CVE2023-20027 vulnerability is in the implementation of the IPv4 Virtual Fragmentation Reassembly (VFR) feature of Cisco IOS XE Software.

## III. RESEARCH METHODOLOGY

In this study, the most recent and significant literature on Moving Target Defense Techniques and Vulnerabilities in Network Switches has been reviewed using the PRISMA (Preferred Reporting Items for Systematic Review and Meta-Analysis) statement [38]. Research publications were found by searching IEEE Xplore, Springer, Science Direct and Elsevier online peer-reviewed databases. This filtration procedure was carried out between February and December 2023.

The selected papers were further screened by reading the abstract. Then considering the subtopics addressed in the Literature Review section, the papers were classified. The papers were reviewed based on the following classifications:

Usage of MTD in Different Applications - In this section, the study was conducted on eleven recent research publications to analyze how the Moving Target Defence concept has been adopted in different applications to defend against various attacks including network reconnaissance.

Other Approaches to Defend Against Net-work Reconnaissance - This section reviews papers that contribute other security mechanisms to defend specifically against network reconnaissance attacks.

Vulnerabilities in Network Switches and Pro-posed Security Solutions -The last section in the Literature Review emphasizes the most important part of this study. Five recent research publications are reviewed that address the vulnerabilities in network switches by proposing different security solutions.

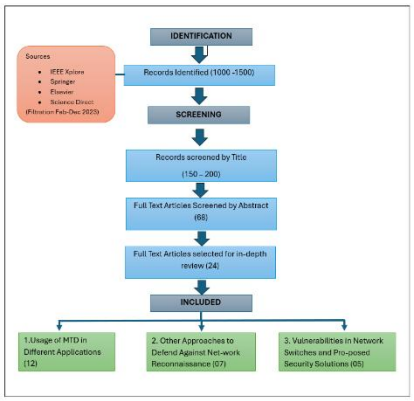



Fig.2 PRISMA Flow Diagram: Paper Selection and Screening Process.

The aforementioned areas help find the application of MTD techniques in switch port reconnaissance attacks (i.e. port scanning) in recent research. The review then is analyzed to find the research gaps in the addressed area from this paper.

## IV. ANALYSIS AND DISCUSSION

Table I summarizes the first section of the literature review. It reveals a trend towards using Moving Target Defense (MTD) techniques to defend against various cyberattacks. Three studies focus on employing dynamic network configurations (specifically IP randomization) within the MTD concept. Two of these three studies, authored by E. Al-Shaer, target the network reconnaissance phase.

Al-Shaer proposes an IP randomization technique to specifically counter reconnaissance attacks. While this approach can mitigate the threat of port scanning, IP addresses remain discoverable through other methods. These alternative methods exploit the inherent advantages attackers have with IP addresses: their widespread recognition and prevalence compared to other network configurations.

Examples of such techniques include social engineering, DNS spoofing, targeting Internet of Things (IoT) devices, and harvesting information from public leaks or website visitor tracking. Unlike IP addresses, other network configurations like port numbers, subnet masks, and MAC addresses are generally less understood by the public.

Furthermore, Moving Target Defense (MTD) techniques are finding application in the increasingly

popular technology of Software-Defined Networks (SDNs). These techniques offer defense against various attacks, including Crossfire attacks and Blind DDoS attacks. MTD relies on different randomization mechanisms to enhance security. While MTD has become a common security approach in SDNs, there remains significant potential to explore MTD-based solutions against port scanning attacks.

TABLE I. ANALYSIS OF DIFFERENT MTD TECHNIQUES APPLIED IN THE IN THE RECENT LITERATURE

| Research | MTD Technique | Attacks Defended |
|---|---|---|
| [14] | change the parameters of a system dynamically and constantly | sensor, actuator attacks |
| [15] | switching supervisory control between sensors | sensor deception attacks |
| [16] | detector entry switching | stealthy sensor attacks |
| [17] | changes the IP address and routes in a network | reconnaissance, DoS attacks, and Botnet attacks |
| [18] | assigning virtual IP addresses that change randomly | reconnaissance, DoS attacks, and Botnet attacks |
| [20] | IP randomization | DDoS attacks |
| [21] | optimal randomization | |
| [22] | route randomization which reduces the link flooding | Crossfire attacks |
| [23] | changes the SDN controller dynamically | Blind DDoS attacks |
| [24] | randomly assign virtual IP addresses to cover the real ones | |
| [25], [26] | IP shuffling and host mutating | |

The second section of the literature review examines alternative approaches for securing Software-Defined Networks (SDNs), focusing on monitoring and detection systems proposed in recent research. These studies explore solutions that leverage technologies beyond Moving Target Defense (MTD).

In Table II, it summarizes the vulnerabilities discovered in network switches. One proposed solution act as a mechanism to overcome compromised switches in Software-Defined Networks (SDNs) by isolating the identified compromised ones. However, this technique, which involves changing the network topology, can still be labor-intensive and potentially introduce new configuration errors. Even with Intrusion Detection Systems (IDS) in place, modern reconnaissance techniques like slow port scanning can still pose a threat. Table II highlights several solutions proposed by researchers to address vulnerabilities at switch ports. These solutions include developing new testing address them. mechanisms for protocols, creating robust security policies specifically for switch ports, and implementing a dedicated server to provide network security services.

Additionally, it emphasizes the current threats targeting switchports, including the mechanisms that attackers exploit.

TABLE II. SUMMARY THE VULNERABILITIES DISCOVERED IN NETWORK SWITCHES

| Research | Vulnerability | Proposed Solution |
|---|---|---|
| [33] | Compromised switches | Changing network topology |
| [34] | VLAN's logical separation | Intruder Detection |
| [35] | Long strings before authentication, buffer overflow in parameter fields | Mutation based fuzz testing |
| [36] | Private VLAN (PVLAN) vulnerabilities | Switching security policies |
| [37] | VLAN hopping attacks, Private VLAN vulnerabilities, Spanning-Tree Protocol vulnerabilities, CAM table overflow attacks, DHCP starvation attacks, and MAC spoofing attacks | AAA Server |

## V. CONCLUSION AND FURTHER RESEARCH

This paper thoroughly analyzes existing vulnerabilities in switchports and how recent researcher-proposed solutions address them. Additionally, it emphasizes the current threats targeting switchports, including the mechanisms that attackers exploit.

The reconnaissance phase of an attack is crucial, as it provides attackers with vital information about the target network. Network scanning is the primary technique used in this phase, encompassing various port scanning methods. Slow port scans are a modern threat, particularly challenging to mitigate even with popular solutions like Intrusion Detection Systems (IDS).

This study makes a significant contribution by identifying connections and applications between Moving Target Defense (MTD) techniques and switchport vulnerabilities. The analysis reveals two key findings. First, existing solutions defend against switchport threats using techniques other than MTD. Second, MTD itself can be incorporated into network security mechanisms. Additionally, the literature review suggests a gap in research regarding MTD applications for mitigating port scanning threats. The literature review suggests a gap in research regarding MTD applications for mitigating port scanning threats. Future work should focus on developing practical MTD implementation scenarios, such as integrating dynamic VLAN/port randomization policies directly into SDN controllers or designing hybrid MTD-firewall systems to provide a proactive defense against reconnaissance and scanning.

REFERENCES


[1] W. Gragido and J. Pirc, “9 - Seven Commonalities of Subversive Multivector Threats,” in Cybercrime and Espionage, W. Gragido and J. Pirc, Eds., Boston: Syngress, 2011, pp. 153–175. doi: 10.1016/B978-1-59749-613-1.00009-1.

[2] S. A. Shaikh, H. Chivers, P. Nobles, J. A. Clark, and H. Chen, “Network reconnaissance,” Netw. Secur., vol. 2008, no. 11, pp. 12–16, Nov. 2008, doi: 10.1016/S1353-4858(08)70129-6.

[3] L. Wang and D. Wu, “Moving Target Defense Against Network Reconnaissance with Software Defined Networking,” in Information Security, M. Bishop and A. C. A. Nascimento, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2016, pp. 203–217. doi: 10.1007/978-3-319-45871-7_13.

[4] W. H. Allen, G. A. Marin, and L. A. Rivera, “Automated detection of malicious reconnaissance to enhance network security,” in Proceedings. IEEE SoutheastCon, 2005., Apr. 2005, pp. 450–454. doi: 10.1109/SECON.2005.1423286.

[5] W. Mazurczyk and L. Caviglione, “Cyber reconnaissance techniques,” Commun. ACM, vol. 64, no. 3, pp. 86–95, Feb. 2021, doi: 10.1145/3418293.

[6] M. I. Al-Saleh, Z. A. Al-Sharif, and L. Alawneh, “Network Reconnaissance Investigation: A Memory Forensics Approach,” in 2019 10th International Conference on Information and Communication Systems (ICICS), Jun. 2019, pp. 36–40. doi: 10.1109/IACS.2019.8809084.

[7] P. Pandey, “Prevention of ARP spoofing: A probe packet based technique,” in 2013 3rd IEEE International Advance Computing Conference (IACC), Feb. 2013, pp. 147–153. doi: 10.1109/IAdCC.2013.6514211.

[8] M. Dabbagh, A. J. Ghandour, K. Fawaz, W. E. Hajj, and H. Hajj, “Slow port scanning detection,” in 2011 7th International Conference on Information Assurance and Security (IAS), Dec. 2011, pp. 228–233. doi: 10.1109/ISIAS.2011.6122824.

[9] M. u Nisa and K. Kifayat, “Detection of Slow Port Scanning Attacks,” in 2020 International Conference on Cyber Warfare and Security (ICCWS), Oct. 2020, pp. 1–7. doi: 10.1109/ICCWS48432.2020.9292389.

[10] C. Lei, H.-Q. Zhang, J.-L. Tan, Y.-C. Zhang, and X.-H. Liu, “Moving Target Defense Techniques: A Survey,” Secur. Commun. Netw., vol. 2018, pp. 1–25, Jul. 2018, doi: 10.1155/2018/3759626.

[11] S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang, Eds., Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats, vol. 54. in Advances in Information Security, vol. 54. New York, NY: Springer New York, 2011. doi: 10.1007/978-1-4614-0977-9.

[12] T. Yadav and A. M. Rao, “Technical Aspects of Cyber Kill Chain,” in Security in Computing and Communications, J. H. Abawajy, S. Mukherjea, S. M. Thampi, and A. Ruiz-Martínez, Eds., in Communications in Computer and Information Science. Cham: Springer International Publishing, 2015, pp. 438–452. doi: 10.1007/978-3-319-22915-7_40.

[13] N. Saputro, S. Tonyali, A. Aydeger, K. Akkaya, M. A. Rahman, and S. Uluagac, “A Review of Moving Target Defense Mechanisms for Internet of Things Applications,” in Modeling and Design of Secure Internet of Things, John Wiley & Sons, Ltd, 2020, pp. 563–614. doi: 10.1002/9781119593386.ch24.

[14] A. Kanellopoulos and K. G. Vamvoudakis, “A Moving Target Defense Control Framework for Cyber-Physical Systems,” IEEE Trans. Autom. Control, vol. 65, no. 3, pp. 1029–1043, Mar. 2020, doi: 10.1109/TAC.2019.2915746.

[15] R. Meira-Góes and S. Lafortune, “Moving Target Defense based on Switched Supervisory Control: A New Technique for Mitigating Sensor Deception Attacks11The work of R.M.G. and S.L. was supported in part by US NSF grants CNS-1738103 and CNS-1801342.,” IFAC-Pap., vol. 53, no. 4, pp. 317–323, Jan. 2020, doi: 10.1016/j.ifacol.2021.04.031.

[16] D. Umsonst, S. Saritaş, and H. Sandberg, “A Nash equilibrium-based moving target defense against stealthy sensor attacks,” in 2020 59th IEEE Conference on Decision and Control (CDC), Dec. 2020, pp. 3772–3778. doi: 10.1109/CDC42340.2020.9304197.

[17] E. Al-Shaer, “Toward Network Configuration Randomization for Moving Target Defense,” in Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats, S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang, Eds., in Advances in Information Security. , New York, NY: Springer, 2011, pp. 153–159. doi: 10.1007/978-1-4614-0977-9_9.

[18] E. Al-Shaer, Q. Duan, and J. H. Jafarian, “Random Host Mutation for Moving Target Defense,” in Security and Privacy in Communication Networks, A. D. Keromytis and R. Di Pietro, Eds., in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Berlin, Heidelberg: Springer, 2013, pp. 310–327. doi: 10.1007/978-3-642-36883-7_19.

[19] J. H. Jafarian, E. Al-Shaer, and Q. Duan, “An Effective Address Mutation Approach for Disrupting Reconnaissance Attacks,” IEEE Trans. Inf. Forensics Secur., vol. 10, no. 12, pp. 2562–2577, Dec. 2015, doi: 10.1109/TIFS.2015.2467358.

[20] N. Bandi, H. Tajbakhsh, and M. Analoui, “FastMove: Fast IP switching Moving Target Defense to mitigate DDOS Attacks,” in 2021 IEEE Conference on Dependable and Secure Computing (DSC), Jan. 2021, pp. 1–7. doi: 10.1109/DSC49826.2021.9346278.

[21] A. Clark, K. Sun, and R. Poovendran, “Effectiveness of IP address randomization in decoy-based moving target defense,” in 52nd IEEE Conference on Decision and Control, Dec. 2013, pp. 678–685. doi: 10.1109/CDC.2013.6759960.

[22] A. Aydeger, N. Saputro, K. Akkaya, and M. Rahman, “Mitigating Crossfire Attacks Using SDN-Based Moving Target Defense,” in 2016 IEEE 41st Conference on Local Computer Networks (LCN), Nov. 2016, pp. 627–630. doi: 10.1109/LCN.2016.108.

[23] D. Ma, Z. Xu, and D. Lin, “Defending Blind DDoS Attack on SDN Based on Moving Target Defense,” in International Conference on Security and Privacy in Communication Networks, J. Tian, J. Jing, and M. Srivatsa, Eds., in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Cham: Springer International Publishing, 2015, pp. 463–480. doi: 10.1007/978-3-319-23829-6_32.

[24] J. H. Jafarian, E. Al-Shaer, and Q. Duan, “Openflow random host mutation: transparent moving target defense using software defined networking,” in Proceedings of the first workshop on Hot topics in software defined networks, in HotSDN ’12. New York, NY, USA: Association for Computing Machinery, Aug. 2012, pp. 127–132. doi: 10.1145/2342441.2342467.

[25] J. Narantuya et al., “SDN-Based IP Shuffling Moving Target Defense with Multiple SDN Controllers,” in 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks – Supplemental Volume (DSN-S), Jun. 2019, pp. 15–16. doi: 10.1109/DSN-S.2019.00013.

[26] D. C. MacFarland and C. A. Shue, “The SDN Shuffle: Creating a Moving-Target Defense using Host-based Software-Defined Networking,” in Proceedings of the Second ACM Workshop on Moving Target Defense, in MTD ’15. New York, NY, USA: Association for Computing Machinery, Oct. 2015, pp. 37–41. doi: 10.1145/2808475.2808485.

[27] C. Birkinshaw, E. Rouka, and V. G. Vassilakis, "Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks," J. Netw. Comput. Appl., vol. 136, pp. 71–85, Jun. 2019, doi: 10.1016/j.jnca.2019.03.005.

[28] S. Liu, M. K. Reiter, and V. Sekar, "Flow Reconnaissance via Timing Attacks on SDN Switches," in 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Jun. 2017, pp. 196–206. doi: 10.1109/ICDCS.2017.281.

[29] T. Shimanaka, R. Masuoka, and B. Hay, Cyber Deception Architecture: Covert Attack Reconnaissance Using a Safe SDN Approach. 2019. Accessed: Sep. 04, 2022. [Online]. Available: http://hdl.handle.net/10125/60166

[30] 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 Trans. Netw. Serv. Manag., vol. 14, no. 4, pp. 1098–1112, Dec. 2017, doi: 10.1109/TNSM.2017.2724239.

[31] Zal, M., Michalski, M., & Zwierzykowski, P. (2024). Implementation of a Lossless Moving Target Defense Mechanism. *Electronics*, *13*(5), 918.

[32] Lima, R. A. F. D., Lemos, M. E. R. G. Q., & Junior, J. A. F. S. (2023). Low delay network attributes randomization to proactively mitigate reconnaissance attacks in industrial control systems. *Wireless Networks*, *30*(6), 1–15.

[33] N. C. Thang and M. Park, "An efficient defense method for compromised switch and middlebox-bypass attacks in service function chaining," J. Commun. Netw., vol. 22, no. 6, pp. 493–504, Dec. 2020, doi: 10.23919/JCN.2020.000028.

[34] S. Thapliyal, H. Gupta, and S. K. Khatri, "An Intruder Monitoring System for Improving the Network Security," in 2019 4th International Conference on Information Systems and Computer Networks (ISCON), Nov. 2019, pp. 26–31. doi: 10.1109/ISCON47742.2019.9036195.

[35] X. Han, Q. Wen, and Z. Zhang, "A mutation-based fuzz testing approach for network pro{Citation}tocol vulnerability detection," in Proceedings of 2012 2nd International Conference on Computer Science and Network Technology, Dec. 2012, pp. 1018–1022. doi: 10.1109/ICCSNT.2012.6526099.

[36] S. A. Alabady, F. Al-Turjman, and S. Din, "A Novel Security Model for Cooperative Virtual Networks in the IoT Era," Int. J. Parallel Program., vol. 48, no. 2, pp. 280–295, Apr. 2020, doi: 10.1007/s10766-018-0580-z.

[37] S. A. J. Alabady, "Design and Implementation of a Network Security Model using Static VLAN and AAA Server," in 2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications, Apr. 2008, pp. 1–6. doi: 10.1109/ICTTA.2008.4530276.

[38] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement," Ann. Intern. Med., vol. 151, no. 4, pp. 264–269, Aug. 2009, doi: 10.7326/0003-4819-151-4-200908180-00135.