Caliphate Journal of Science & Technology (CaJoST)

ISSN: 2705-313X (**PRINT**); 2705-3121 (**ONLINE**) **Research Article**

Open Access Journal available at: https://cajost.com.ng/index.php/files and https://www.ajol.info/index.php/cajost/index

DOI: https://dx.doi.org/10.4314/cajost.v7i1.01

Article Info

Received: 27th April 2024

Revised: 6th December 2024

Accepted: 20th January, 2025

Department of Electrical and Computer Engineering, Kwara State University, Kwara State, Nigeria.

***Corresponding author's email:**

bilkisu.jimada@kwasu.edu.ng

Cite this: *CaJoST*, 2025, 1, 1-11

Security Analysis in Wireless Networks

Muheez A. Rahim, Bilkisu Jimada-Ojuolape, Monsurat O. Balogun, Lambe M. Adesina

Wireless networks have become essential to our daily lives, providing connectivity for a wide range of devices. However, with the increasing use of wireless networks, security has become a major concern. Media Access Control (MAC) address flooding, Dynamic Host Configuration Protocol (DHCP) spoofing, and rogue Secure Shell (SSH) are some of the most common security threats in wireless networks. These attacks can cause loss of confidentiality, integrity, and availability of network resources. In this study, vulnerabilities and challenges related to MAC address flooding, DHCP spoofing, and rogue SSH attacks were investigated. Analysis of the solution to prevent and mitigate these attacks was performed by network simulation using the Cisco Packet Tracer Windows version 8.1.1. The system design would provide a user-friendly interface for network administrators to monitor their networks and check for anomalies. The analysis indicated that Port Security effectively limited unauthorized MAC addresses, DHCP snooping successfully blocked illegitimate DHCP responses, and Access Control Lists restricted rogue SSH access, supporting these methods as optimal solutions for mitigating the respective security threats.

Keywords: Cyber-attack, Flooding, Network security, Spoofing, Wireless Networks.

1. Introduction

Wireless network security Analysis is an examination of methods and techniques for detecting and mitigating security issues faced by wireless networks worldwide [1]. The use of wireless networks is immensely increasing daily as it is now becoming the fastest and most efficient way of communicating and storing information globally. Security is a vital concern in wireless applications, especially as individuals increasingly depend on wireless networks to transmit sensitive information, such as credit card transactions and banking communications[2]. A wireless network utilizes radio signals to transmit data between multiple physical devices, commonly referred to as 'nodes' within the network [3]. There are several ways that people, organizations, and the government communicate wirelessly, with satellite communication being the primary form. There is also infrared communication, radio transmission, microwave communication, Wi-Fi, mobile communication systems, and Bluetooth technology [4].

The main purpose of network security is to ensure that information on the network is well protected [5]. Network security encompasses the fundamental perspectives or viewpoints individuals hold regarding issues related to securing networks[6]. The importance of safeguarding network data and ensuring its sensitivity is fundamental to establishing secure communication across systems [7]. It possesses the following characteristics: integrity, confidentiality, and availability. Basically, from a standard perspective, a network must have the integrity to ensure that all digital information stored on it is accurate and must be safeguarded against accidental damage or modification. Subsequently, to ensure that digital information assets are accessible to the users for whom the advertisement is intended, confidentiality must be guaranteed. Finally, a secure network must guarantee the availability of digital information assets to authorized users when needed, without exclusion. Network security is a critical concern for organizations of all sizes [8]. The population of connected devices and the increasing reliance on computer networks have made the most significant challenge in network security the threat of network-based network resources and disruption of network operations. A network environment is typically vulnerable to a variety of security threats[9]. This research will focus on three specific network security problems: Media Access Control (MAC) address flooding, Dynamic Host Configuration Protocol (DHCP) spoofing, and

rogue Secure Shell (SSH). MAC address flooding is a type of network attack that involves flooding a network with fake MAC addresses to exhaust the available address space [10]. This can cause network congestion, slow down performance, and even cause the network to crash. The second attack which is DHCP spoofing is a type of attack in which an attacker sends fake DHCP responses to a client, providing the client with false Internet Protocol (IP) addresses and other network configuration information [11]. This can allow the attacker to intercept your network traffic and gain unauthorized access to the network. Lastly, a rogue SSH server is a malicious SSH server configured by an attacker to intercept legitimate SSH connections [12]. This can allow the attacker to gain unauthorized access to the network and steal sensitive information.

In the 21st century, technological progress has led to heightened data security risks, including data theft and misuse, particularly in organizations handling sensitive information, prompting the necessity for robust network security measures. With the emergence of early electronic computers, the challenges of network security began to surface, prompting global attention to the need for effective governance to address vulnerabilities and safeguard interconnected systems [13]**.** In 2017, cyberattacks like the WannaCry ransomware outbreak highlighted how malicious software can severely disrupt essential services, affecting critical sectors such as healthcare and government operations [14]. Ransomware attacks have increasingly posed a severe threat to enterprises and government agencies by leveraging advanced encryption techniques that make data recovery difficult, leading to substantial financial losses, prolonged operational downtime, and widespread disruptions in critical sectors, highlighting the urgent need for stronger security measures within wireless networks, as vulnerabilities such as weak encryption, unsecured access points, and lack of network segmentation can serve as potential entry points for these cyber threats, ultimately reinforcing the importance of implementing robust wireless security strategies to mitigate risks and enhance overall network resilience [15]. Information system occupies a very important position in any organization or government by the data and information that it contains. Thus, this study investigates vulnerabilities and challenges related to MAC address flooding, DHCP spoofing, and rogue SSH attacks, and also analyses solutions to prevent and mitigate these attacks. The rest of the article is outlined as follows: section 2 highlights an empirical review of the considered attacks, section 3 discusses the research methods including a system design and implementation, and section 4 outlines the results and discusses the findings from each attack investigation. Lastly, the paper is concluded in section 5.

2. Review of Related Works

In [16] MAC address attacks are classified as masquerade attacks, resource exhaustion attacks, or media access attacks in IEEE 802.11 networks. Masquerade Attack refers to an attack in which an opponent targets a specific client by spoofing its MAC address or the address of its current access point. Resource Exhaustion Attack refers to an attack in which an attacker generates high rates of requests with random MAC addresses to consume shared resources. Finally, media access attacks refer to attacks against the Distributed Coordinated Function (DCF) of 802.11 networks. These attacks are also called jamming attacks. However, the authors proposed a MAC address spoof detection method to counter these attacks. The MAC address spoof detection method is based on a sequence number field whose value is increased by one for each unfragmented frame. An attacker cannot change the value of the sequence number because they generally cannot control the functionality of their wireless card's firmware. By analyzing the sequence number patterns of captured wireless traffic, detection systems Show the ability to detect MAC address spoofing to identify de-authentication/disconnection attacks.

Authors in [10] explain how to authenticate using the Authentication, Authorization, and Accounting (AAA) server to reduce MAC address flooding. An AAA server is a program that processes user access requests to computer resources and provides authentication, authorization, and accounting services for a company. Authentication is the process of identifying a MAC address, usually based on availability in the MAC address table. Authorization is the process of granting or denying a user access to network resources after authentication is complete. Accounting is the process of tracking activity when accessing network resources, including time spent on the network. The proposed approach to mitigate this uses a direct digital signal between the source and destination through authentication and authorization. The target knows the public key of the source. A digital signature can be formed by encrypting the entire message with the sender's private key by encrypting a hash. Message code containing the sender's private key.

In study [17], the authors introduce a project aimed at mitigating DHCP attacks. The lack of message authentication on the DHCP server makes it vulnerable to attacks such as DHCP starvation attacks and spoofing. A DHCP starvation attack

occurs when attackers flood a DHCP server with requests for IP addresses making IP addresses unavailable to legitimate users. The proposed approach to counteract these attacks is DHCP snooping. It is configured on a network switch and works by listening to all communications on the network. A database known as the DHCP binding database is maintained and constantly populated with clients' DHCP-assigned addresses, their MAC addresses, access ports, and Virtual Local Area Networks (VLANs). a package that is different from the one stored in the database, omit the Packets, which maintain the security of the DHCP server.

The study by [11] performed some testing on the DHCP server, made some observations, and discovered a vulnerability in the DHCP server that has the potential for DHCP rogue or DHCP spoofing, causing all clients to fail to communicate with the authorized DHCP server as well as open the gateway for attackers to penetrate the network. However, the proposed method to mitigate this was to implement DHCP snooping and DHCP snooping methods. DHCP snooping ensures that all traffic has been filtered and directed to the registered interface. DHCP alerts are required to monitor traffic during the Discovery, Offer, Request, and Acknowledgment (DORA) process. In tests conducted, DHCP snooping and DHCP alerts successfully anticipated attacks attempting to inject rogue DHCP into the network infrastructure. The DHCP alert configured on the proxy router ensures that the DORA process can only take place between an authorized DHCP server and a client. The DHCP snooping test also shows that client communications can only be answered by a trusted DHCP server. With the presence of DHCP Snooping and DHCP Alert, the host configuration is fully controlled by the authorized DHCP server.

The research in [18] verified existing credentials using network dictionaries to prevent SSH and FTP brute force attacks. They consider standard usernames (like admin, administrator, or device names) and generic username schemes (first and last name combinations) to be two groups worth including in these dictionaries. They also allude to the Rock You incident that exposed 32,603,388 user credentials in 2009. Although the initial exploit took advantage of a trivial Structured Query Language (SQL) injection vulnerability, it provides valuable clues about preferred passwords. A dictionary attack based on the top 5,000 passwords would result in a 0.9% hit rate.

In the article [19], the study examined brute force SSH attacks performed on six college campus networks using honeypot techniques. Brute-force password-guessing attacks against SSH, FTP, and Telnet servers are the most common form of attacks to compromise Internet-facing servers. A key factor in avoiding disruption to these networks is defending them against brute force attacks. Evidence shows that pre-compiled lists of widely used usernames and passwords form the basis of brute-force attacks. The analysis of passwords found that in the case of actual malicious traffic, what is commonly understood as a strong password does not protect systems from compromise. The data evaluated from the study uses the expiration and regeneration of SSH keys periodically to protect the system against these attacks. The main reason to change your private key is when you have reason to believe it has been compromised or is no longer secure.

Authors in [20] used Unsupervised Machine Learning and Association Rule Mining (ARM) algorithms to model, visualize and interpret the behavior of SSH brute force attacks. They decide against supervised and semi-supervised machine learning because of the cost of tagged traffic for their hands-on training. The analysis of this article supports the hypothesis that the behavior of SSH brute force attacks differs significantly from that of normal SSH sessions.

The authors in [21] suggested using Continuous Auditing (CAUDIT) of SSH servers to mitigate brute-force attacks against them. Its concept aims to automatically isolate hosts on a production network that happen to be vulnerable to such crimes. That's why its developers present an SSH-based honeypot with a tempting full-class B network that henceforth mimics a realistic 64,000-machine server farm. results in immediate source IP address blacklisting and destination node isolation as no authorized user would attempt to access either of the two attractive Class B IP addresses from positive authentication, CAUDIT blacklists, and quarantines in case of stolen credentials.

2.1 Literature Review Table

Reference	Focus of Study	Identified Threats	Proposed Solution	Key Findings
[16]	Classification of MAC address attacks in IEEE 802.11 networks	- Masquerade attacks - Resource exhaustion attacks - Media access (jamming) attacks	MAC address spoof detection based on sequence number tracking	Sequence number analysis can detect spoofing in wireless traffic, aiding in identifying de-authentication and disconnection attacks
[10]	Authentication for MAC address flooding prevention	- MAC address flooding	Use of AAA (Authentication, Authorization, Accounting) server with digital signals for authentication	AAA server provides authentication, authorization, and accounting, reducing MAC address flooding by verifying MAC addresses.
[17]	Mitigating DHCP starvation and spoofing attacks	- DHCP starvation - DHCP spoofing	DHCP snooping on network switches	DHCP snooping effectively filters unauthorized requests and maintains a binding database for client information, ensuring DHCP server security.
[11]	Testing and mitigation of DHCP server vulnerabilities	- DHCP rogue - DHCP spoofing	DHCP snooping with alerts for monitoring DORA processes	DHCP snooping and alert configuration ensure only authorized DHCP communications occur, preventing unauthorized access.
[18]	Credential verification to prevent SSH and FTP brute-force attacks	- SSH brute-force attacks - FTP brute-force attacks	Use of network dictionaries with common usernames and password patterns	Network dictionaries and top password lists enable early detection of brute-force attacks by identifying commonly exploited credentials.
[19]	Examination of brute-force SSH attacks with honeypot techniques	- Brute-force attacks on SSH, FTP, and Telnet	SSH key expiration and regeneration	Regular renewal of SSH keys prevents brute-force success even against strong passwords.
[20]	Unsupervised ML and ARM for SSH brute-force behavior analysis	- SSH brute-force attacks	Modeling with Unsupervised Machine Learning and Association Rule Mining	Unsupervised ML highlights behavioral differences between normal and attack traffic, aiding SSH brute-force detection.
[21]	Continuous auditing (CAUDIT) of SSH servers for brute-force mitigation	- SSH brute-force attacks	SSH honeypot with IP blacklisting and node isolation	CAUDIT approach blacklists suspicious IPs and quarantines destination nodes, effectively isolating potential threats from legitimate traffic.

3. Materials and Methods

Following a comprehensive review of the methods and techniques used in this research. It establishes theoretical views and empirical research techniques on network security to assemble a set of components to develop a network security vulnerability assessment framework for MAC address flooding, DHCP spoofing, and unauthorized SSH, using a case study model to apply appropriate research methodologies highlighted in the System Implementation section that ensure the achievement of the objectives of the research.
The proposed simulation software for the research design is the Cisco Packet Tracer**.**

3.1 System Design

This section describes the process of defining the system architecture and, interfaces to meet the specified requirements. A network design model was applied to this research to develop

the framework. Figure 1 shows an architectural overview of how the system works and the flow of interactions for different processes. Figure 2 shows the major interactions between the different actors in the network security vulnerability analysis framework.

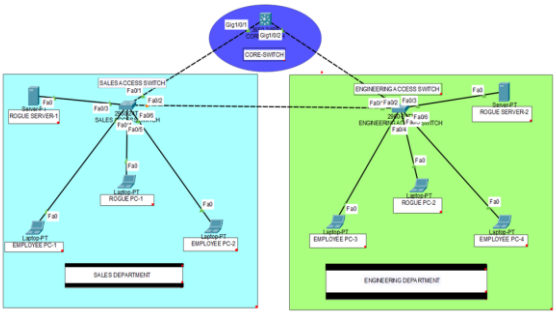

Figure 1: Network Design Model.

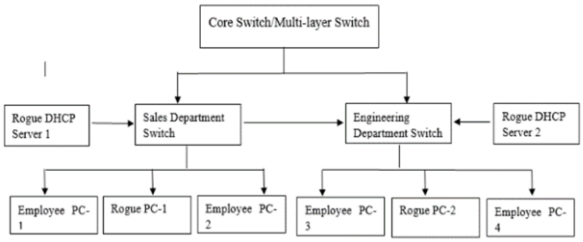

Figure 2: Block Diagram of The Proposed Network Design

3.2. System Implementation

3.2.1. MAC Address Flooding

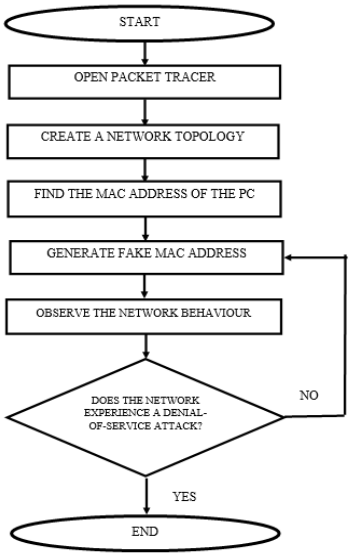

Figure 3a: Flow Chart of the steps for simulating MAC address Flooding.

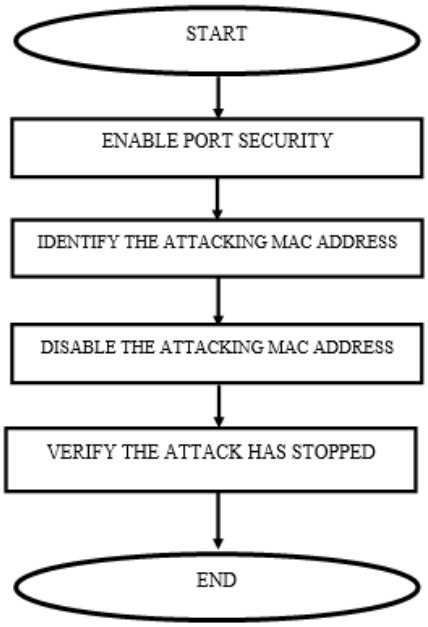

Figure 3b: Flow chart of the steps for stopping MAC Address Flooding

3.2.2. DHCP Spoofing

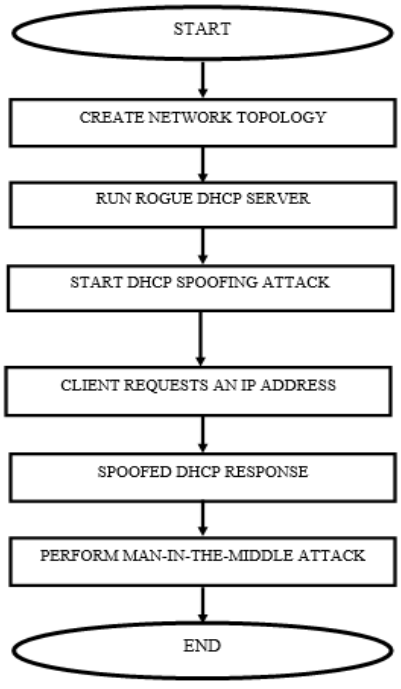

Figure 4a: Flow chart of the steps for simulating DHCP Spoofing.

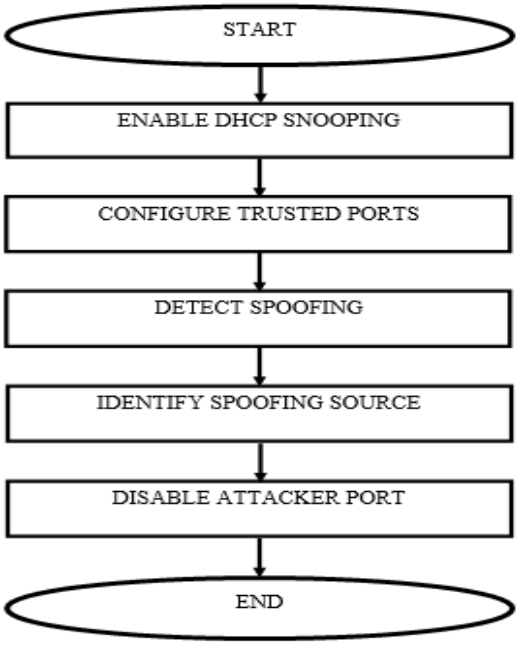

Figure 4b: Flow Chart of the Steps to simulate stopping the DHCP Spoofing

4. Results and Analysis

This section shows the results of simulating the network security problems; MAC address flooding, DHCP Spoofing, and Rogue SSH using Packet Tracer. Additionally, the effectiveness of implementing the mitigation measures will be explored.

4.1. MAC Address Flooding

The attack involved generating a significant number of fake MAC addresses using the Python programming language, which the Rogue PCs later modified by changing their configuration settings on the Packet Tracer. **Figure 7** shows Rogue PC-1 modifying the fake MAC addresses, the same process was repeated by Rogue PC-2. It was observed that the MAC address flooding from the Rogue PCs overwhelmed the MAC address tables of the Sales and Engineering access switches. As a result, incomplete MAC address entries typically represented by a hyphen (-) or other symbol, appeared in the tables. This behavior is consistent with the characteristics of a MAC address flooding attack, where the switches can no longer learn and store all legitimate MAC addresses.

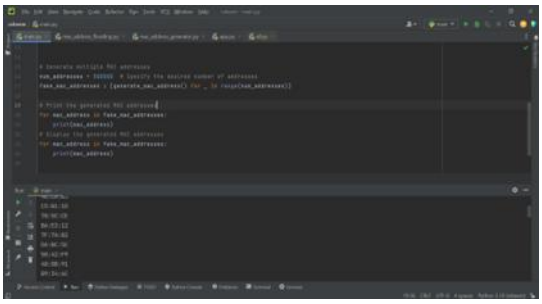

Figure 6: Fake MAC Addresses generated with Python programming language.

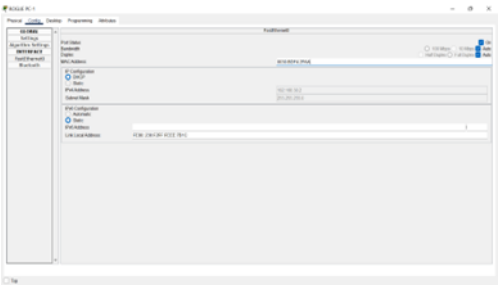

Figure 7: Rogue PC-1 modifying the fake MAC addresses in packet tracer.

Figure 8: MAC address flooding ongoing on the Sales access switch.

Figure 9: MAC address flooding successful on the sales access switch.

4.1.1 Mitigation

The MAC address flooding attack mitigation required a series of prompt actions. First, the ports connected to the Rogue PCs responsible for the flooding were immediately disabled. **Figure 12** shows the port connected to Rogue PC-1 has been disabled, the same process was repeated for Rogue PC-2. This immediate response severed the network connection for the offending devices. After disabling the ports, the next step was to clear the MAC

address table on the access switches. By doing so, all existing fake MAC address entries were successfully removed. This allowed the switches to relearn and store legitimate MAC addresses accurately, restoring the proper functioning of the MAC address table. To enhance network security and prevent future flooding attacks, port security was enabled on all ports connecting the hosts. This measure played a crucial role in the mitigation efforts. By setting a maximum limit on the number of MAC addresses allowed and defining authorized MAC addresses for each port, the switches effectively restricted the ability of unauthorized devices to flood the network with fake MAC addresses. This additional layer of security helped prevent any future disruptions caused by flooding attacks.

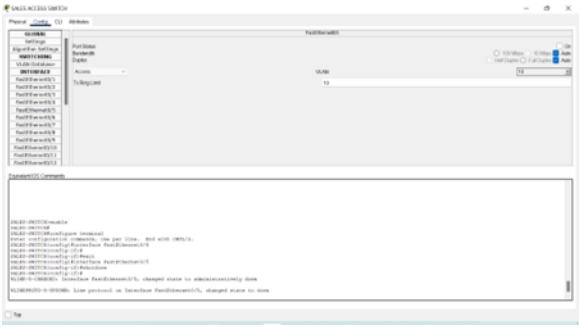

Figure 10: Ports connected to the Rogue PC-1 disabled.

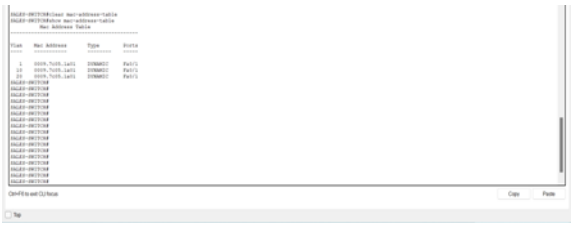

Figure 11: MAC address table for the sales access switch cleared.

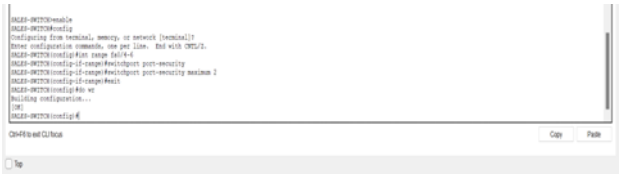

Figure 12: Port security enabled on all ports connecting the hosts on the sales access switch

4.2 DHCP Spoofing

This attack involves two Rogue DHCP servers, Rogue server-1 in the sales department and Rogue server-2 in the engineering department sending false DHCP packets to the hosts in each department. It was observed that when the Rogue servers spoofed the DHCP server's responses, they could trick the hosts in each department into obtaining rogue DHCP packets like incorrect IP addresses, default gateways, and DNS servers. This malicious activity disrupted the normal network operations and will potentially allow the Rogue servers to redirect traffic to malicious destinations.

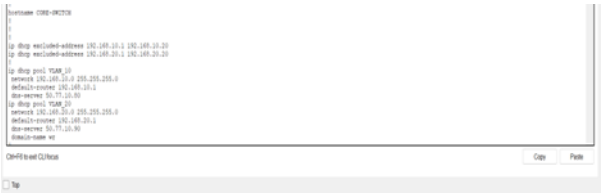

Figure 13: Legitimate DHCP server packets.

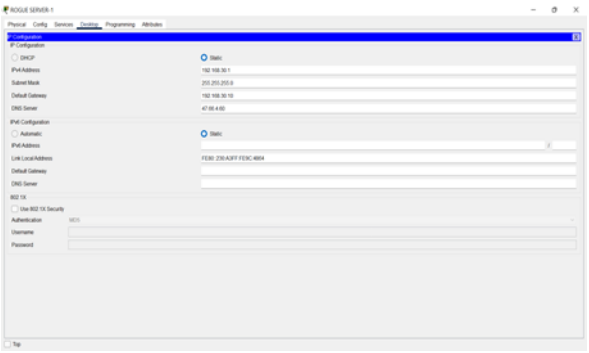

Figure 14: Rogue server-1 DHCP packets.

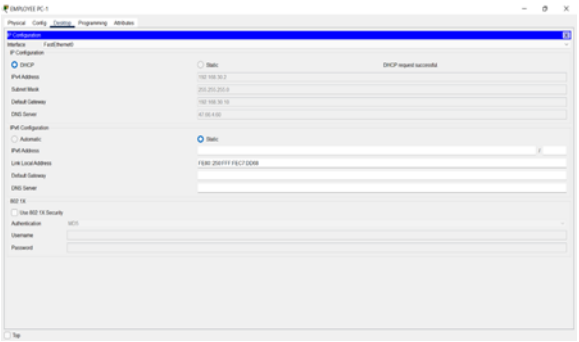

Figure 15: Sales department host after requesting for DHCP packets.

The rogue server-1 intercepts the Core Switch's message, which is the legitimate server, and sends rogue packets to the sales department host.

4.2.1 Mitigation

To mitigate DHCP spoofing, DHCP snooping was implemented on the sales access switch and the engineering access switch. DHCP snooping is a security feature that validates DHCP messages exchanged between hosts and the DHCP server. It ensures that only trusted DHCP server responses are accepted by the hosts. As a result, when the rogue servers sent their spoofed DHCP responses, the DHCP snooping feature detected the unauthorized messages and dropped them. The hosts were then prevented from receiving unauthorized IP addresses, and other DHCP packets, maintaining network integrity and security.

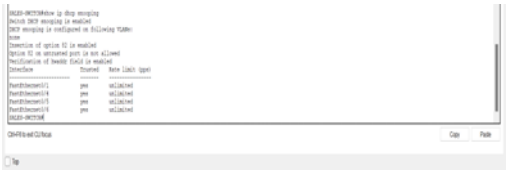

Figure 16: DHCP Snooping has taken effect on the Sales access switch.

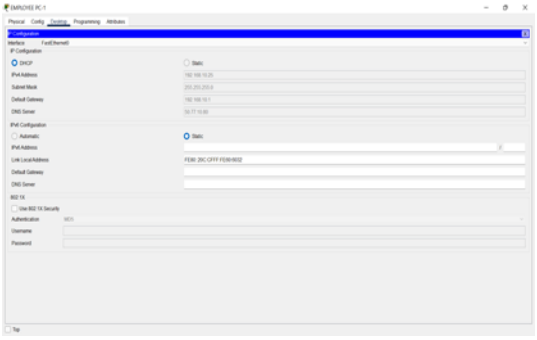

Figure 17: Sales department host after DHCP Snooping has taken effect.

4.3 Rogue SSH

Rogue SSH connections pose a significant risk to network security, as they enable unauthorized access to critical resources. In this project, it was established that only hosts from the engineering department have authorized access to SSH connections. Conversely, hosts from the sales department lack proper authorization, making their SSH connections a potential breach of network security. Unauthorized SSH connections can compromise sensitive information and jeopardize the overall integrity of the network. The detection of rogue SSH connections has significant implications for network security. It was observed that hosts from the sales department were able to gain unauthorized access to SSH connections on both the access switches and the multilayer switch. Network monitoring and analysis played a crucial role in the identification of these rogue SSH connections. By examining network logs and analyzing traffic patterns, the presence of unauthorized access attempts could be determined. The detection of these rogue connections highlighted potential security breaches within the network infrastructure.

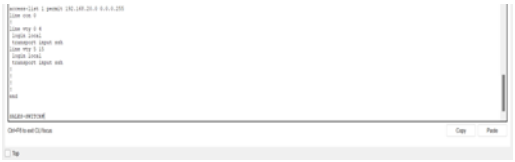

Figure 18: Only the Engineering department hosts have authorized access to SSH connections.

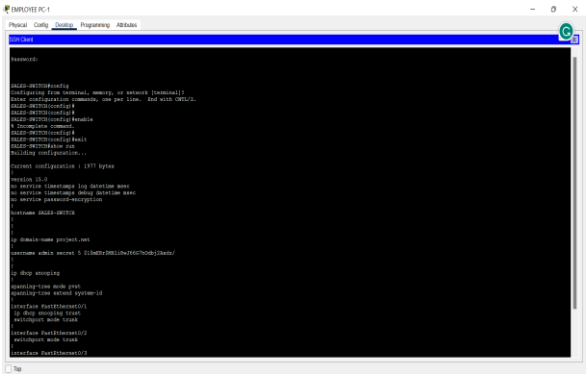

Figure 19: The sales department hosts unauthorized access to SSH connections via the sales access switch

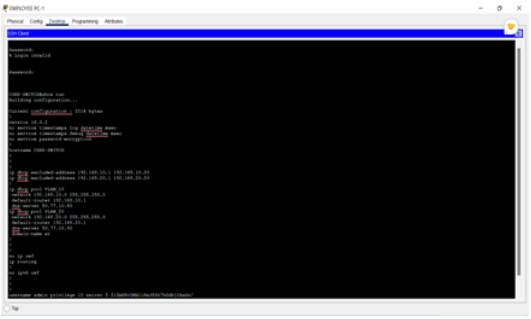

Figure 20: Sales department host unauthorized access to SSH connections via Core switch.

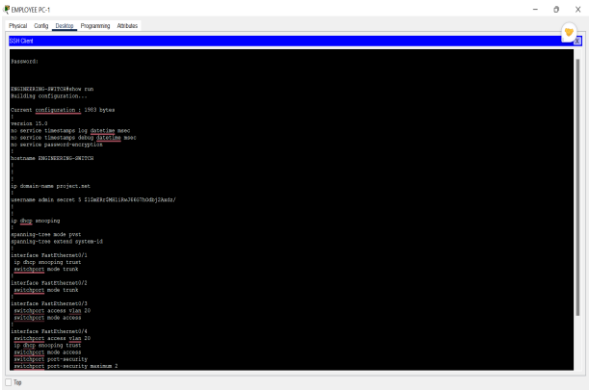

Figure 21: Sales department host unauthorized access to SSH connections via the Engineering switch.

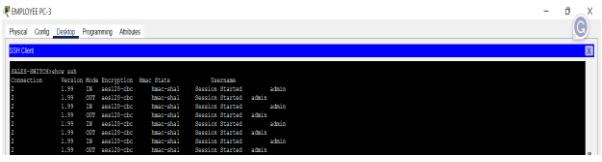

Figure 22: Rogue SSH connection showing on the sales access switch.

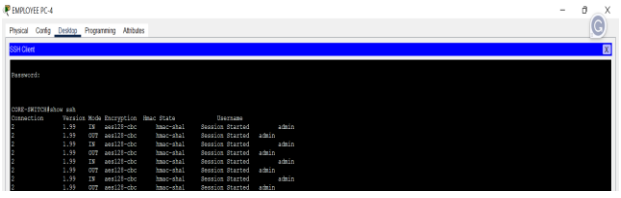

Figure 23: Rogue SSH connection showing on the Core switch.

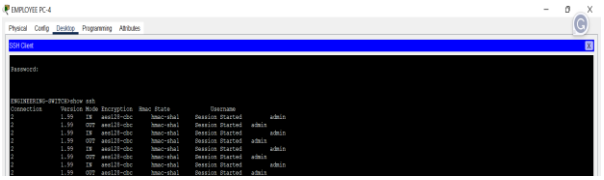

Figure 24: Rogue SSH connection showing on the engineering access switch.

4.3.1 Mitigation

The rogue SSH connections were mitigated by applying Access Control Lists (ACLs) on both the sales and engineering access switches, as well as the core switch. ACL provides a mechanism to control network traffic by defining rules that permit or deny specific types of traffic based on criteria such as IP address, and protocol. ACLs were configured on the access switches to control SSH access to the network. The rules were defined to allow SSH connections only from authorized IP addresses associated with the engineering department while denying SSH connections from the sales department. By enforcing these ACLs on the access switches, the network was protected from unauthorized SSH access attempts. ACLs were also implemented on the multilayer switch. Similar to the access switches, the ACLs on the multilayer switch were configured to permit SSH connections only from authorized IP addresses associated with the engineering department. All other SSH connection attempts were denied, preventing unauthorized access to the network resources.

Figure 25: ACL activated on the sales department to authorize only the engineering hosts.

Figure 26: ACL activated on the core switch to authorize only the engineering hosts.

Figure 27: ACL activated on the engineering access switch to authorize only the engineering hosts.

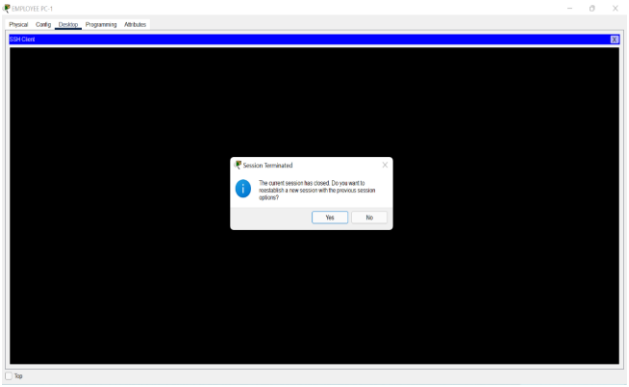

Figure 28: Sales department host unable to access SSH connections after ACL has been activated on the sales access switch.

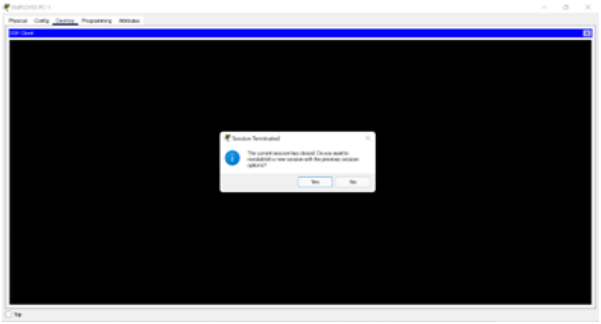

Figure 29: Sales department host unable to access SS connections after ACL has been activated on the core switch.

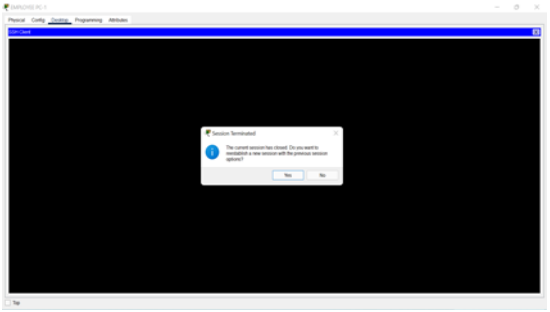

Figure 30: The sales department host unable to access SSH connections after ACL has been activated on the engineering access switch.

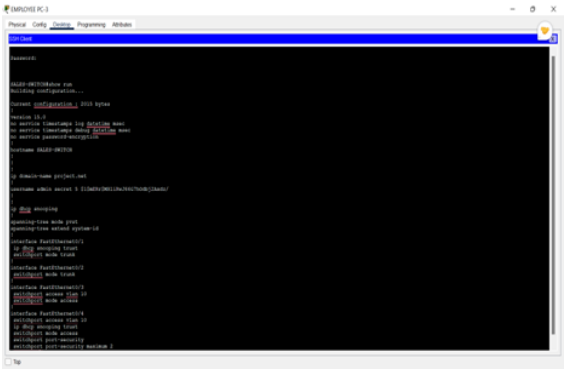

Figure 31: Engineering department host able to access SSH connections after ACL has been activated on the sales access switch.

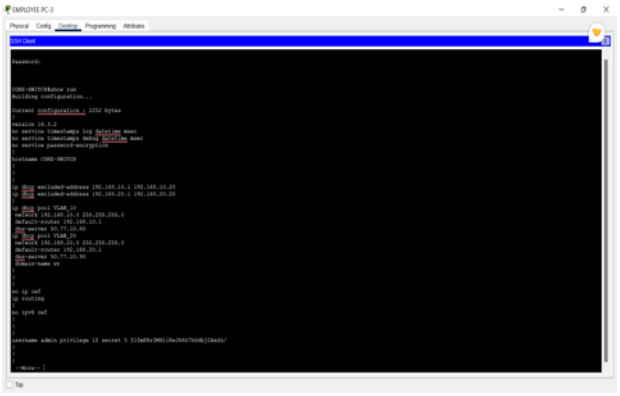

Figure 32: Engineering department host able to access SSH connections after ACL has been activated on the core switch.

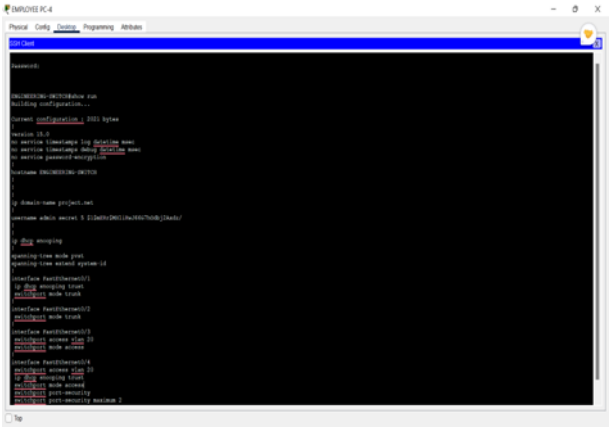

Figure 33: Engineering department host able to access SSH connections after ACL has been activated on the engineering access switch.

5. Conclusion

This research investigated the effects of the network security problems: MAC address flooding, DHCP spoofing, and Rogue SSH and their respective mitigation strategies highlighting the importance of taking proactive measures to ensure network security and integrity. The mitigation strategies employed include shutting down ports and enabling port security for MAC address flooding, implementing DHCP snooping for DHCP spoofing, and applying ACLs for rogue SSH connections, effectively mitigating the risks associated with these network security threats. The successful implementations of those strategies ensure a secure network environment, prevent unauthorized access, maintain network performance, and protect sensitive information.

Conflict of interest

The authors declare no conflict of interest.

Acknowledgement

The authors thank all involved in the realisation of this article.

References

[1] R. Nazir, A. A. laghari, K. Kumar, S. David, and M. Ali, “Survey on Wireless Network Security,” May 01, 2022, *Springer Science and Business Media B.V.* doi: 10.1007/s11831-021-09631-5.

[2] F. B. Schneider, “Viewpoint: Impediments with policy interventions to foster cybersecurity,” *Commun ACM*, vol. 61, no. 3, pp. 36–38, Mar. 2018, doi: 10.1145/3180493.

[3] R. Di Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, “Security in wireless ad-hoc networks - A survey,” Sep. 15, 2014, *Elsevier*. doi: 10.1016/j.comcom.2014.06.003.

[4] M. Islam and S. Jin, “An Overview Research on Wireless Communication Network,” *Advances in Wireless Communications and Networks*, vol. 5, no. 1, p. 19, 2019, doi: 10.11648/j.awcn.20190501.13.

[5] N. Threats and A. A. S. Measures, “NETWORK THREATS, ATTACKS AND SECURITY MEASURES: A REVIEW,” *International Journal of Advanced Research in Computer Science*, vol. 8, no. 8, 2017, doi: 10.26483/ijarcs.v8i9.4641.

[6] Y.-S. , Shiu, S. , Chang, H.-C. , Wu, S. , Huang, and H.-H. Chen, “Physical layer security in wireless networks: a tutorial,” *IEEE Wirel Commun*, vol. 18, no. 2, pp. 66–74, Apr. 2011, doi: https://doi.org/10.1109/MWC.2011.5751298.

[7] E. Toch *et al.*, “The privacy implications of cyber security systems: A technological survey,” Jul. 31, 2018, *Association for Computing Machinery*. doi: 10.1145/3172869.

[8] S. Youn, “Analysis of security protocols in wireless sensor networks,” *ICIC Express Letters, Part B: Applications*, vol. 11, no. 11, 2020, doi: 10.24507/icicelb.11.11.1087.

[9] M. G. Rahman and H. Imai, “Security in Wireless Communication,” *Wirel Pers Commun*, vol. 22, pp. 213–228, Sep. 2002, doi: https://doi.org/10.1023/A:1019968506856.

[10] S. M. P. Nair and Akhila L, “MAC flooding Attack Prevention with Machine Learning,” *Journal of Engineering, Computing and Architecture*, vol. 10, no. 2, pp. 114–120, 2020, doi: DOI:17.0002.JECA.2020.V10I2.200786.4909.

[11] D. A. Pradana and A. S. Budiman, “The DHCP Snooping and DHCP Alert Method in

Securing DHCP Server from DHCP Rogue Attack," *IJID (International Journal on Informatics for Development)*, vol. 10, no. 1, pp. 38–46, Jun. 2021, doi: 10.14421/ijid.2021.2287.

[12] G. Salles-Loustau, R. Berthier, E. Collange, B. Sobesto, and M. Cukier, "Characterizing attackers and attacks: An empirical study," in *Proceedings of IEEE Pacific Rim International Symposium on Dependable Computing, PRDC*, 2011, pp. 174–183. doi: 10.1109/PRDC.2011.29.

[13] X. Liu, "Design of Wireless Communication Base Station Monitoring System Based on Artificial Intelligence and Network Security," in *Procedia Computer Science*, Elsevier B.V., 2023, pp. 1254–1261. doi: 10.1016/j.procs.2023.11.097.

[14] A. Djenna, D. E. Saidouni, and W. Abada, "A pragmatic cybersecurity strategies for combating IoT-cyberattacks," in *2020 International Symposium on Networks, Computers and Communications, ISNCC 2020*, Institute of Electrical and Electronics Engineers Inc., Oct. 2020. doi: 10.1109/ISNCC49221.2020.9297251.

[15] P. , Bajpai, A. K. , Sood, and R. Enbody, "A key-management-based taxonomy for ransomware," in *2018 APWG Symposium on Electronic Crime Research (eCrime)*, IEEE, May 2018. doi: https://doi.org/10.1109/ECRIME.2018.8376213.

[16] D. Llewellyn-Jones, M. Merabti, and T. Farooq, "MAC Layer DoS Attacks in IEEE 802.11 Networks," Jan. 2010, [Online]. Available: https://www.researchgate.net/publication/266467295

[17] A. Nuhu, F. Oluwatosin Echobu, O. Olanrewaju, N. A. Abdulhafiz, E. O. Faith, and O. M. Oyenike, "MITIGATING DHCP STARVATION ATTACK USING SNOOPING TECHNIQUE MITIGATING DHCP… MITIGATING DHCP STARVATION ATTACK USING SNOOPING TECHNIQUE," *FJS FUDMA Journal of Sciences (FJS*, vol. 4, no. 1, pp. 560–566, 2020, [Online]. Available: https://www.researchgate.net/publication/362773309

[18] R. Mcdougall, N. Gillespie, and D. Guster, "'Using An Enhanced Dictionary to Facilitate Auditing Techniques Related to Brute Force SSH and FTP Attacks,'" 2011. [Online]. Available: https://micsymposium.org/mics_2011_proceedings/mics2011_submission_10.pdf

[19] E. Kheirkhah, S. Mehdi, P. Amin, H. A. Sistani, and H. Acharya, "An Experimental Study of SSH Attacks by using Honeypot Decoys," *Indian J Sci Technol*, vol. 6(12), pp. 5567–5578, Dec. 2013, doi: DOI:10.17485/ijst/2013/v6i12.8.

[20] C. , Yao, X. , Luo, and A. N. Zincir-Heywood, "Data analytics for modeling and visualizing attack behaviors: A case study on SSH brute force attacks," in *SSCI : 2017 IEEE Symposium Series on Computational Intelligence : November 27, 2017-December 1, 2017*, IEEE, Feb. 2018. doi: https://doi.org/10.1109/SSCI.2017.8280913.

[21] P. M. Cao *et al.*, "CAUDIT: Continuous Auditing of SSH Servers to Mitigate Brute-Force Attacks," in *Proceedings of the 16th USENIX Symposium on Networked Systems Design and Implementation (NSDI '19) : Boston, MA, USA, February 26 - 28, 2019*, USENIX Association, Feb. 2019. [Online]. Available: https://www.usenix.org/system/files/nsdi19-cao.pdf

