Enhancing Local Area Network Security Through Penetration Testing and Port Security

Mariam A. Emsaad, Motaz M. Al Shaba, Malik M. Farhat

Department of Computer Networks, University of Tripoli, Libya

m.emsaad@uot.edu.ly
malekfarhat06@gmail.com
DOI: https://10.5281/zenodo.18114791

Abstract. Local Area Networks (LANs) remain highly vulnerable to protocol-based attacks that exploit weaknesses in essential network services. Among the most common attacks are Dynamic Host Configuration Protocol (DHCP) starvation, Address Resolution Protocol (ARP) spoofing, and Virtual Local Area Network (VLAN) hopping, which can severely compromise network confidentiality, integrity, and availability. This study investigates the effectiveness of penetration testing in identifying and mitigating such vulnerabilities within LAN environments. A simulated network was designed using GNS3, and controlled attacks were executed using Kali Linux and the Yersinia toolset to evaluate network resilience. Based on the penetration testing results, vulnerabilities were identified and mitigated using a single security mechanism, namely Port Security. The experimental results demonstrate that applying Port Security significantly reduced the number of successful attacks and improved overall network security. The findings highlight the importance of penetration testing as a practical approach for enhancing LAN security and provide cost-effective recommendations suitable for small and medium-sized organizations.

Keywords: Cyber-attacks, Penetration Testing, DHCP Starvation, ARP Spoofing, VLAN Hopping, Port Security.

1 Introduction.

Cybersecurity has become a critical concern for modern organizations due to the rapid growth of network-based services and the increasing sophistication of cyber-attacks. Local Area Networks (LANs), which form the core infrastructure of most organizations, are particularly exposed to attacks that exploit vulnerabilities in fundamental network protocols. Attacks such as Dynamic Host Configuration Protocol (DHCP) starvation, Address Resolution Protocol (ARP) spoofing, and Virtual Local Area Network (VLAN) hopping are among the most prevalent threats targeting LAN environments. These attacks can result in unauthorized access, traffic interception, denial of service, and the compromise of sensitive information [1]. Cybercrime poses multifaceted challenges to individuals, organizations, and societies, necessitating concerted efforts in

research, policy, and technology to mitigate risks and enhance cybersecurity resilience. Scientific literature underscored the importance of continuous vigilance, collaboration, and innovation in addressing evolving cyber threats and safeguarding digital ecosystems [2]. The primary goal of network security is to prevent unauthorized access, data breaches, and cyberattacks that can compromise sensitive information, disrupt operations, and lead to financial losses [3].

This study addresses the following research question:

- What are the most common vulnerabilities in local area networks, and how can penetration testing help mitigate them?

Accordingly, the main objective of this research is to assess the effectiveness of penetration testing in discovering and mitigating vulnerabilities associated with DHCP, ARP, and VLAN protocols. To achieve this objective, a controlled experimental environment is established in which real-world attacks are simulated using Kali Linux and the Yersinia penetration testing tool.

The significance of this research lies in providing practical and low-cost security recommendations that can be easily adopted by small and medium-sized organizations. By demonstrating how penetration testing can identify critical weaknesses and how a single mitigation technique—Port Security—can substantially reduce successful attacks, this study contributes to improving the security and resilience of local area network infrastructures.

2 The Importance of Cybersecurity

Cybersecurity plays a fundamental role in protecting network infrastructures against a wide range of threats that target data, services, and communication systems. With the increasing reliance on Local Area Networks (LANs) to support organizational operations, any weakness in network security mechanisms can lead to unauthorized access, service disruption, or data compromise. As a result, cybersecurity has become a critical requirement rather than an optional enhancement for modern networks.

From a technical perspective, effective cybersecurity aims to preserve the confidentiality, integrity, and availability of network resources. Attacks targeting core network protocols, such as DHCP starvation, ARP spoofing, and VLAN hopping, directly undermine these security objectives by enabling traffic interception, manipulation of network communications, and denial of essential services. Such attacks are particularly dangerous in LAN environments, where internal trust assumptions and misconfigurations are often exploited.

Penetration testing provides a practical and cost-effective approach to cybersecurity by simulating realistic attack scenarios and evaluating the resilience of network configurations under controlled conditions. By analyzing how networks respond to common protocol-based attacks, security administrators can validate existing defenses, identify misconfigurations, and apply targeted mitigation techniques. Consequently, cybersecurity is not limited to deploying security mechanisms but also requires continuous testing and validation to ensure that network infrastructures remain resilient against evolving

threats. The importance of Cybersecurity stems from three main axes, shown in Fig.1 below:

Fig. 1. CIA with Cyber Security [4]

2.1 Confidentiality, Integrity, and Availability (CIA Triad)

The security of local area networks is fundamentally evaluated through the Confidentiality, Integrity, and Availability (CIA) triad, which represents the core objectives of information security. In LAN environments, protocol-based attacks primarily target weaknesses in these objectives rather than exploiting application-level vulnerabilities.
Confidentiality is compromised when attackers gain unauthorized access to network traffic or sensitive information. Attacks such as ARP spoofing enable adversaries to intercept and monitor data exchanges between legitimate hosts, allowing the disclosure of credentials and private communications. Similarly, VLAN hopping undermines traffic isolation mechanisms, enabling attackers to access restricted network segments that are intended to be logically separated [5,6].
Integrity refers to the assurance that data and network communications are not altered without authorization. In the context of LAN attacks, integrity violations occur when malicious entities manipulate protocol messages or routing information to redirect traffic or inject false data. ARP spoofing attacks, for instance, allow attackers to modify address resolution mappings, leading to man-in-the-middle scenarios where transmitted data can be altered without detection [5,6].
Availability ensures that network services and resources remain accessible to authorized users when required. Protocol-based attacks such as DHCP starvation directly target availability by exhausting network resources, preventing legitimate devices from obtaining IP addresses and joining the network. These attacks can result in service outages and operational disruption, particularly in environments that rely on dynamic address allocation [5-7].

Given the direct impact of DHCP, ARP, and VLAN-related attacks on the CIA triad, protecting LAN infrastructures requires security mechanisms that enforce strict access control and limit unauthorized protocol interactions. Consequently, assessing and strengthening these mechanisms through penetration testing is essential to maintaining a balanced and resilient security posture that addresses all three CIA objectives.

3 Types of Cybersecurity

Cybersecurity encompasses multiple domains that collectively aim to protect information systems, networks, and digital assets from evolving threats. Rather than treating these domains as isolated components, effective security strategies integrate them to address risks across different layers of the network infrastructure.

Network security focuses on protecting communication channels, devices, and protocols from unauthorized access and misuse. In local area networks, this domain is particularly critical, as protocol-level vulnerabilities can be exploited to intercept traffic, disrupt services, or bypass logical segmentation mechanisms. Attacks such as DHCP starvation, ARP spoofing, and VLAN hopping highlight the importance of enforcing robust network security controls at both Layer 2 and Layer 3.

In this study, the focus is placed on network security due to its direct relevance to protocol-based attacks within LAN infrastructures. By evaluating network-level vulnerabilities through penetration testing and applying targeted mitigation techniques, this work demonstrates how strengthening a single cybersecurity domain can significantly enhance overall system security.

The Cybersecurity includes not only traditional IT systems but also the security of emerging technologies like the Internet of Things (IoT), cloud computing, and artificial intelligence [8]. The types of cyber-Security: Network Security. Application Security. Cloud Security. Internet Security and Endpoint Security [9].

4 Cybersecurity attacks

Cyber-attacks are any attacks involving digital technologies, such as computer networks or the internet, to gain access to systems, manipulate data, or disrupt or disable them [10]. Malware is responsible for many of the Distributed Denial-of-Service (DDoS) attacks as well as spam and phishing activities [11].Cyber-attacks encompass a wide range of types and methods that attackers can use, including as shown in Fig.2.

Fig. 2. Types of Cyber Attacks [10].

5 Cybersecurity Tools

Cybersecurity tools play a crucial role in detecting, analyzing, and mitigating security threats within computer networks. Rather than providing absolute protection, these tools support security administrators by offering visibility into network behavior and enabling timely responses to suspicious activities. Their effectiveness depends largely on how well they are integrated into the overall security strategy.

In local area network environments, cybersecurity tools are commonly used to monitor traffic patterns, identify abnormal protocol behavior, and evaluate the impact of security controls. Penetration testing tools, in particular, allow security practitioners to simulate realistic attack scenarios and assess the resilience of network configurations against known vulnerabilities. This proactive approach enables the identification of weaknesses that may not be detected through passive monitoring alone.

In this study, penetration testing was conducted using specialized tools capable of exploiting protocol-level vulnerabilities relevant to LAN infrastructures. The selected tools were used to generate controlled DHCP starvation, ARP spoofing, and VLAN hopping attacks, providing practical insight into how these threats affect network operations. Traffic analysis tools were also employed to observe attack behavior and validate the effectiveness of mitigation mechanisms.

Various Cybersecurity tools are designed to counter specific threats. Here are some of the most popular Cybersecurity tools shown in Fig.3 [9].

Fig. 3. Types of Cybersecurity Tools [9].

6 Authentication and Authorization

Authentication is security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to

receive specific categories of information, authentication assures secure systems, secure processes and enterprise information security, authenticating a user involves establishing that the user is in fact who he claims to be [12-14].

Authorization is the process of determining what actions and resources an authenticated user, device, or system is allowed to access or perform [15].

7 Network protocols and Technologies

The design will depend on the requirements that telecommunications companies use in building and designing their networks. Protocols, devices, technologies, and each component in the network will be discussed in this paper.

Local Area Networks rely on a set of fundamental protocols and technologies to enable communication, address allocation, and traffic segmentation. While these mechanisms are designed to improve efficiency and manageability, weaknesses in their configuration can be exploited to launch protocol-based attacks. This section briefly introduces the key protocols and technologies relevant to the experimental evaluation conducted in this study.

Virtual Local Area Networks (VLANs) are used to logically segment a physical network into isolated broadcast domains, improving traffic management and security. However, improper VLAN configuration can allow attackers to bypass segmentation controls. In this work, VLANs serve as the primary mechanism for traffic isolation, making them a critical target for VLAN hopping attacks aimed at gaining unauthorized access to restricted network segments [16-18].

Port security is a feature in computer network protocols that are used to secure access to network ports. It works by assigning a unique media access control (MAC) address to each authorized device that is allowed access to a network port. Port security can be configured in two modes: static and dynamic [19].

Table 1 shows some of the protocols that were used in the paper to transfer data and information over the network securely and efficiently [20].

Table 1. Used Protocols.

Protocol	Identification	Layer
RIPv2	The Routing Information Protocol, version 2 (RIPv2) is an enhanced version of RIP that includes support for important routing features such as class-less addressing and variable-length subnet masks	Layer 3
DHCP	Dynamic Host Configuration Protocol is a protocol used in computer networks to automatically distribute IP addresses and other configuration settings to devices connected to the network.	Layers 2-3

TELNET	The Telnet protocol is based on the Transmission Control Protocol/Internet Protocol (TCP/IP) and uses a specific port to send and receive data between devices	Layer 5

Dynamic Host Configuration Protocol (DHCP) automates the assignment of IP addresses and network parameters to client devices. While DHCP simplifies network administration, it is inherently vulnerable to resource exhaustion attacks. DHCP starvation attacks exploit this weakness by overwhelming the DHCP server with forged requests, thereby preventing legitimate hosts from obtaining network access [21] Fig.4 below shows the DHCP message format [21].

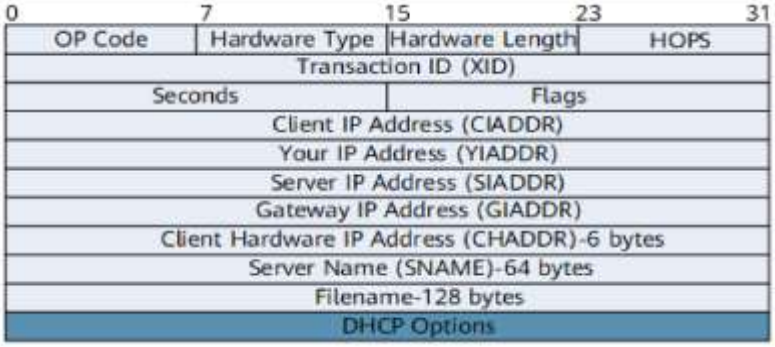

Fig. 4. DHCP Protocol Message Format

Telnet is a protocol for TCP/IP protocols to connect to remote computers, it is also an application for TCP/IPP applications. As show in Fig.5.

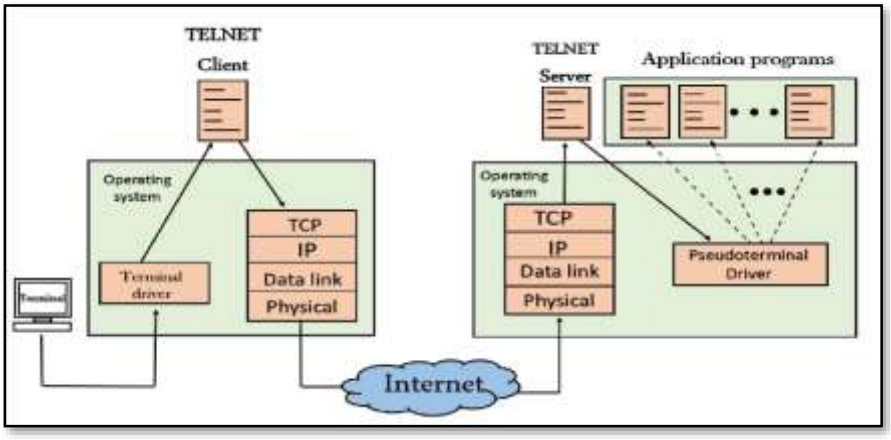

Fig. 5. TELNET Protocol

Address Resolution Protocol (ARP) facilitates the mapping between IP addresses and physical MAC addresses within a local network. Due to its lack of authentication, ARP

is susceptible to spoofing attacks that allow adversaries to manipulate address mappings. Such attacks enable traffic interception and man-in-the-middle scenarios, directly threatening the confidentiality and integrity of network communications.
In addition, Port Security was employed as a defensive mechanism to restrict network access based on authorized MAC addresses and to limit the number of devices per switch port. By enforcing strict access control at the switch level, Port Security reduces the effectiveness of protocol-based attacks and strengthens overall LAN security.
The Routing Information Protocol (RIP) is a distance-vector, interior gateway (IGP) routing protocol used by routers to exchange routing information. RIP uses the hop count as a routing metric [22,23].

8 Methodology

This study adopts an experimental methodology based on controlled penetration testing to evaluate vulnerabilities in local area networks. The objective is to assess the effectiveness of penetration testing in identifying protocol-based attacks and evaluating the impact of mitigation techniques on network security.

8.1 Test Environment

The network environment was simulated using GNS3 to emulate a realistic enterprise local area network. The topology consisted of two switches, two routers, one attacker machine, and one server. The attacker machine was configured with the Kali Linux operating system, while standard routing and switching configurations were applied to ensure normal network operation prior to testing.

Why was Port Security chosen as the sole mitigation mechanism in this study?
Port Security was selected as the sole mitigation mechanism in this study to maintain a focused experimental scope and enable a detailed evaluation of its effectiveness against multiple protocol-based attacks. While several advanced security mechanisms exist, concentrating on a single access control technique allows for a clearer assessment of its impact without introducing additional configuration complexity.

Despite its simplicity, Port Security enforces strict control at the switch level by limiting the number of authorized MAC addresses per port, thereby restricting unauthorized devices from accessing the network. This characteristic makes it particularly relevant for mitigating protocol-based attacks such as DHCP starvation, ARP spoofing, and VLAN hopping, which rely on exploiting unrestricted network access.

Furthermore, Port Security is widely supported by enterprise switches and does not require additional hardware or specialized infrastructure, making it a cost-effective and practical solution for small and medium-sized network environments. The exclusive use of Port Security in this study also highlights its strengths and limitations, providing a foundation for future work that may incorporate complementary security mechanisms such as DHCP Snooping and Dynamic ARP Inspection.

8.2 Penetration Testing Tools

Penetration testing was conducted using the Yersinia framework, which is specifically designed to exploit vulnerabilities in network protocols. Yersinia was selected due to its ability to perform a wide range of Layer 2 and Layer 3 attacks relevant to LAN environments.

8.3 Attack Execution

Three common protocol-based attacks were executed sequentially to assess the network's vulnerability:

1. DHCP Starvation Attack:

This attack was performed to exhaust the available IP address pool on the DHCP server by sending a large number of forged DHCP requests, thereby preventing legitimate clients from obtaining IP addresses.

2. ARP Spoofing Attack:

ARP spoofing was used to intercept network traffic by poisoning the ARP cache of target devices, allowing the attacker to position itself as a man-in-the-middle.

3. VLAN Hopping Attack:

VLAN hopping was executed by crafting IEEE 802.1Q tagged frames to bypass VLAN segmentation and gain unauthorized access to restricted network segments.

8.4 Traffic Monitoring and Data Analysis

Network traffic was monitored using Wireshark to capture and analyze packets during each attack scenario. Abnormal traffic patterns, unauthorized access attempts, and protocol manipulation were recorded both before and after applying security controls.

8.5 Mitigation Technique

After identifying network vulnerabilities, Port Security was implemented on switch interfaces to restrict access based on authorized MAC addresses and limit the maximum number of devices per port. This mitigation technique was selected due to its simplicity, effectiveness, and suitability for small and medium-sized organizations.

9 Network Design

The general network topology consists of two switches, two routers, one attacker and one server. Fig.6 show Network Design.

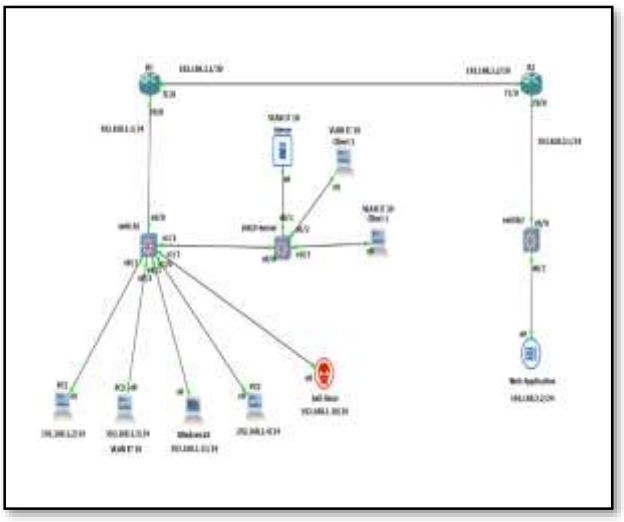

Fig. 6. show Network Design

Attacks used on the network:

- VLAN Hopping: is a cyber-attack to access network resources that are logically isolated on a separate VLAN. By "hopping" to a segment of the network that is supposed to be restricted, the attacker can discover new sensitive systems and data to target. As shown in the Fig.7**.**

Fig. 7. VLAN Hopping

In this step, the attack will be compounded by sending 802.1Q packets targeting VLAN 10, which will enable the attacker to hop between VLANs. As shown in Fig.8,9.

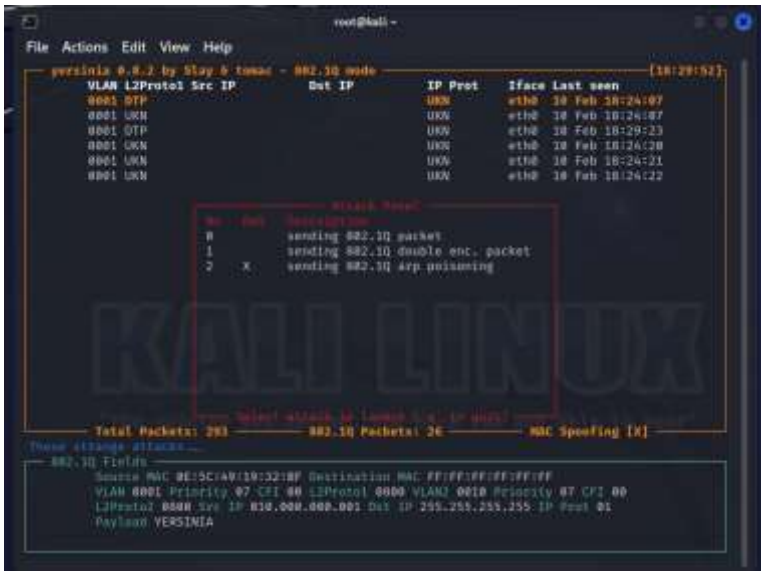

Fig. 8. attack will be compounded by sending 802.1Q packets

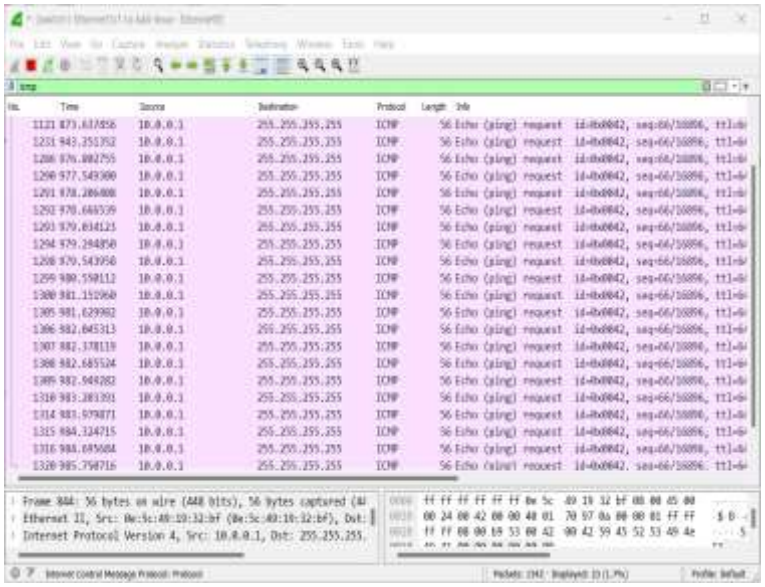

Fig. 9. attacker hop between VLANs

- DHCP starvation: DHCP freeze attack can severely affect IP address distribution in a network and cause disruption to new devices trying to join a network. As shown in the following figs 10,11.

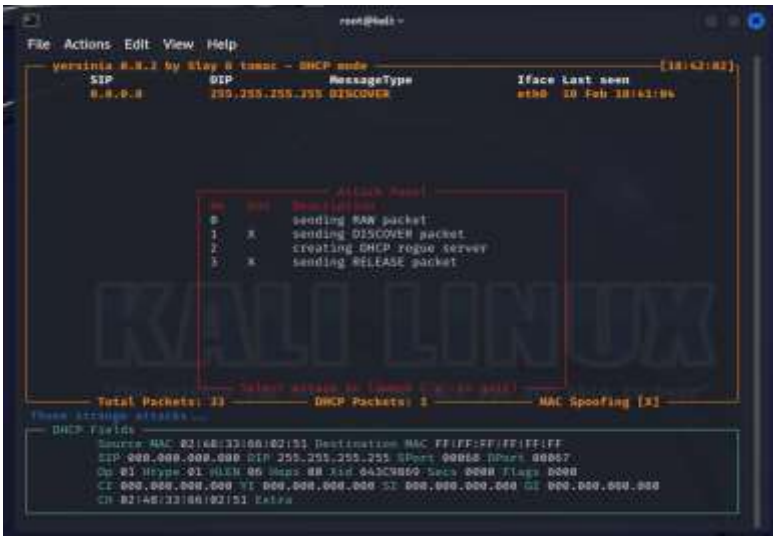

Fig. 10. DHCP freeze attack

Fig. 11. DHCP starvation

- ARP spoofing: Address Resolution Protocol (ARP) spoofing or ARP poisoning is a form of spoofing attack that hackers use to intercept data. A hacker commits an ARP spoofing attack by tricking one device into sending messages to the hacker instead of the intended recipient. As shown in the following figs 12,13.

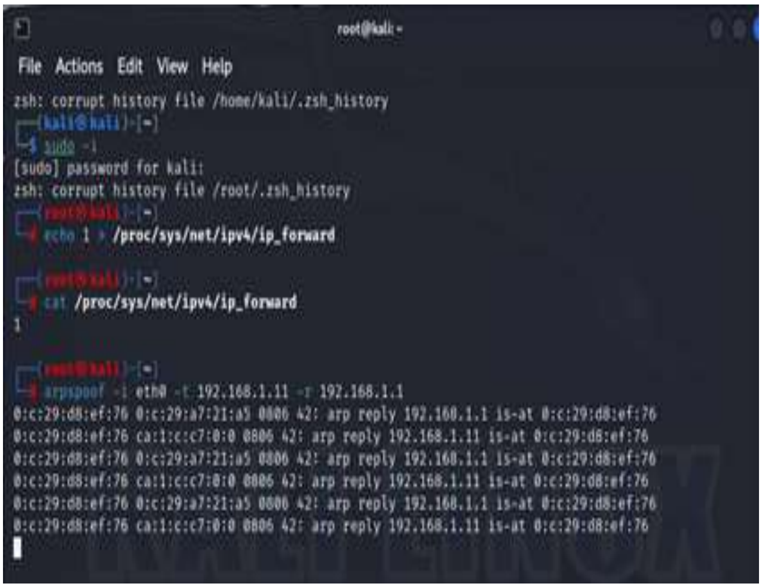

Fig. 12. Spoofing attack

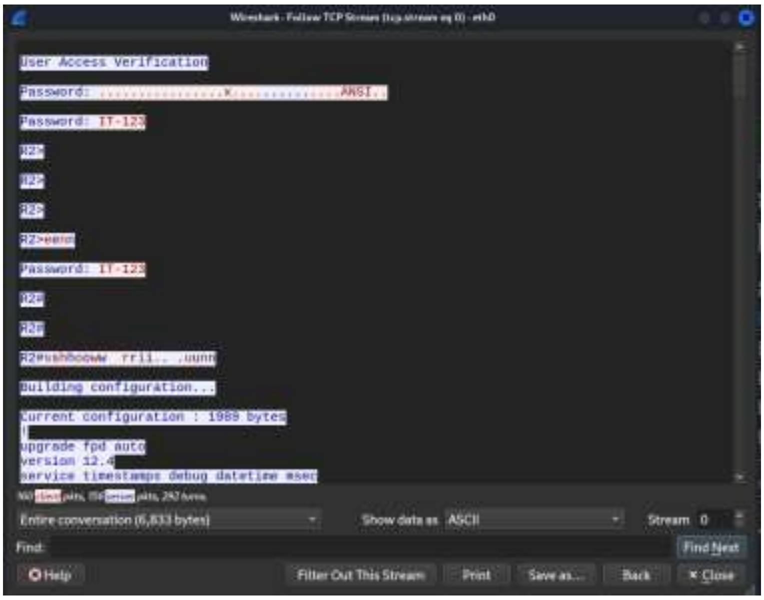

Fig. 13. ARP spoofing

Defense against attacks:

Activating "port security" settings limit the movement on a port based on a set policy. The policy specifies the allowed number of MAC addresses or packages. If there is a breach, the "Port security violation restrict" order identifies the behavior and alerts the official. as shown in Figs.14,15,16.

Fig. 14. Activating "port security".

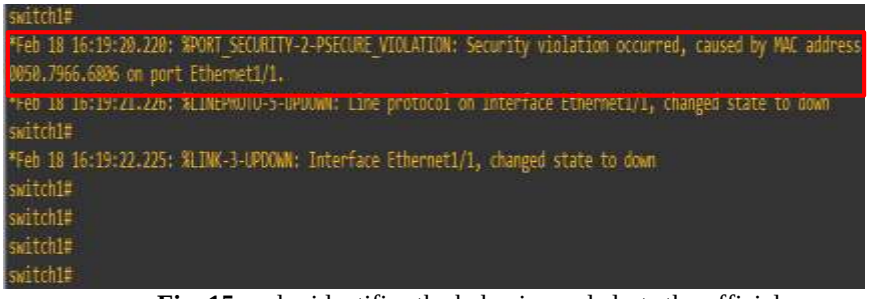

Fig. 15. order identifies the behavior and alerts the official

Fig.16. The policy specifies the allowed number of MAC addresses or packages.

10 Results and Discussion

The penetration testing results revealed several vulnerabilities in the network before the application of security controls. All three attack types—DHCP starvation, ARP spoofing, and VLAN hopping—were successfully executed, indicating weaknesses in protocol configurations and access control mechanisms.

After applying Port Security, a significant reduction in successful attacks was observed.

The results indicate an 80% reduction in successful attacks, demonstrating a substantial improvement in network security. Port Security effectively limited unauthorized device access by enforcing MAC address validation and restricting the number of devices per port.

Port Security was chosen over other mitigation solutions due to its cost-effectiveness, ease of implementation, and minimal hardware requirements. Unlike advanced intrusion detection systems, Port Security can be deployed without additional infrastructure, making it a practical solution for organizations with limited resources.

The experimental results confirm that protocol-based attacks can significantly compromise local area network security when basic access control mechanisms are absent or improperly configured. Prior to the deployment of Port Security, the network environment exhibited a high level of vulnerability to DHCP starvation, ARP spoofing, and VLAN hopping attacks. These findings highlight the extent to which unrestricted device access at the switch level can be exploited to undermine core network operations.

Following the implementation of Port Security, a noticeable reduction in successful attacks was observed across all tested scenarios. This improvement can be attributed to the ability of Port Security to restrict unauthorized devices by enforcing MAC address limitations on switch ports. As a result, attackers were prevented from introducing rogue devices or generating excessive protocol requests, which directly reduced the effectiveness of resource exhaustion and traffic interception attacks.

The results demonstrate that even a single, lightweight security mechanism can provide measurable protection against multiple protocol-based threats when applied correctly. This is particularly relevant for small and medium-sized networks, where complex security solutions may be impractical due to cost or administrative constraints. By focusing exclusively on Port Security, this study was able to isolate its impact and provide a clear assessment of its defensive capabilities without interference from additional security controls.

However, the findings also reveal that Port Security alone does not constitute a comprehensive security solution. While it effectively limits unauthorized access at the switch level, it does not address all attack vectors, particularly those originating from compromised but authorized devices. This limitation underscores the importance of combining Port Security with complementary mechanisms such as DHCP Snooping and Dynamic ARP Inspection in more advanced or large-scale deployments.

Overall, the discussion reinforces the value of penetration testing as a practical approach for validating network security configurations. The observed results emphasize that strategic implementation of simple access control mechanisms can significantly

enhance network resilience, while also highlighting the necessity for layered security in future implementations.

11 Conclusion

This study presented an experimental evaluation of protocol-based attacks in local area networks, focusing on DHCP starvation, ARP spoofing, and VLAN hopping. A realistic LAN environment was simulated using GNS3, where controlled penetration testing was conducted with Kali Linux and the Yersinia framework to assess network vulnerabilities at the protocol level.

The experimental results demonstrated that the examined network was highly susceptible to all three attack types prior to the application of security controls. These findings confirm that misconfigurations and inherent protocol weaknesses can significantly compromise the confidentiality, integrity, and availability of LAN resources. By implementing Port Security as a mitigation technique, a substantial reduction in successful attacks was achieved, indicating a clear improvement in overall network resilience.

One of the key contributions of this work is the demonstration that a single, low-cost security mechanism can effectively mitigate multiple protocol-based attacks when properly configured. Unlike advanced intrusion detection or prevention systems, Port Security can be deployed without additional hardware or complex infrastructure, making it a practical and accessible solution for small and medium-sized organizations.

Overall, this research highlights the importance of penetration testing as a proactive approach to validating network security configurations and identifying critical weaknesses before exploitation occurs. The results emphasize that continuous security assessment, combined with appropriate access control mechanisms, is essential for maintaining secure and reliable local area network infrastructures. Future work may extend this study by evaluating additional mitigation techniques, such as DHCP Snooping and Dynamic ARP Inspection, and by testing the proposed approach in larger and real-world network environments.

Limitations and Future Work

This study focused on a limited network topology and a single mitigation technique. Future research may investigate larger-scale environments, additional security mechanisms, and automated intrusion detection systems to further enhance LAN security.

References

1. Cisco Systems, Cybersecurity, https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html. Accessed 15.1-2024.
2. Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). "*Cybersecurity and cybercrime: Current trends and threats*". Journal of International Studies, 17(2), 220-239. doi:10.14254/2071-8330.2024/17-2/12.

3. TechTarget and Informa , Network security. https://www.techtarget.com/searchnetworking/definition/network-security. Accessed 15.1.2024.
4. Sprint, Cybersecurity, ,https://sprinto.com/blog/importance-of-cyber-security. Accessed date 15.1.2024.
5. hackerone ,Information Security, https://www.hackerone.com/knowledge-center/principles-threats-and-solutions. Accessed 15.1.2024.
6. James Michael Stewart, Ed Tittle, Mike Chapple, " *Certified Information Systems Security Professional* ", Study Guide ,3rd Edition . First edition 2004 SYBEX Inc. Library of Congress Card Number: 2005929270 ISBN: 0-7821-4443-8. 2005 SYBEX Inc., 1151 Marina Village Parkway, Alameda, CA 94501.
7. Tutorialspoint, Availability of Information Security , https://www.tutorialspoint.com/availability-in-information-security. Accessed 15.1.2024.
8. Srisakthi Saravanan , C. V.Suresh Babu." *Cybersecurity: Protecting Information in a Digital World*" April 2024 DOI: 10.4018/979-8-3693-0839-4.ch001. https://www.researchgate.net/publication/380125676 .
9. Acrt ,Authentication methods, https://www.intechopen.com/journals/1/articles/100 authentication authorization accounting. Accessed 17.1.2024.
10. Velásquez I, Caro A, Rodríguez A. Authentication schemes and methods: A systematic literature review. In: *Information and software technology*. Chile: Chillan; 2018. Accessed 17.1.2024.
11. Awais Rashid , Howard Chivers ,George Danezis ,Emil Lupu Imperial , Andrew Martin. "*The CybersecurityBody of Knowledge*".Version 1.0 .31st Oct 2019 https://www:cybok:org/, The National CybersecurityCentre 2019.
12. James Graham, Richard Howard, Ryan Olson." *CYBERSECURITYESSENTIALS*".Auerbach Publications Taylor & Francis Group 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742, 2011 by Taylor and Francis Group, LLC Auerbach Publications is an imprint of Taylor & Francis Group, an Informa business. (Ebook-PDF).
13. Kaine Mathrick , Cybersecurity Framework, https://kmtech.com.au/information-centre/understanding-the-5-types-of-cybersecurity/. Accessed 25.1.2024.
14. Dafydd Stuttard ,Marcus Pinto. "*The Web Application Hacker's Handbook*" . Second Edition. 2011 by Dafydd Stuttard and Marcus Pinto, Published by John Wiley & Sons, Inc., Indianapolis, Indiana.
15. sprinto , Cybersecurity Tool , https://sprinto.com/blog/best-cyber security-tools/. Accessed 25.1.2024.
16. Networkworld ,VLAN Network ,https://www.networkworld.com/article/971100/what-is-a-vlan-and-how-does-it-work.html. Accessed 5.2.2024.
17. Cisco ccna, VLAN, https://study-ccna.com/what-is-a-vlan/ . Accessed 5.2.2024.
18. Oracle server, VLAN Security,https://docs.oracle.com/en/servers/x86/x9-2/security-guide/vlan-security.html#GUID414D4728-2EDC-4F66-AD34-41D3C87BDEFA. Accessed 7.2.2024.
19. Servermania, port security, https://blog.servermania.com/port-security. Accessed 12.2.2024.
20. Cloudzy, TELNET, https://cloudzy.com/blog/telnet-vs-ssh/. Accessed 15.2.2024.
21. Windowstechno ,Dynamic Host Configuration Protocol , https://windowstechno.com/dynamic-host-configuration-protocol-dhcp/. Accessed 15.2.2024.
22. techtarget., Routing Information Protocol, https://www.techtarget.com/searchnetworking/definition/Routing-Information-Protocol. Accessed 18.2.2024.
23. Dan Pei1, Dan Massey 2 and Lixia Zhang." *A Formal Specification for RIP Protocol*", 16.9.2014.

تعزيز أمن الشبكة المحلية من خلال اختبار الاختراق وأمن المنافذ

مريم أبوعجيلة مساعد ، معتز محمد الشبة ، مالك مصطفى فرحات
كلية تقنية المعلومات ، جامعة طرابلس ، ليبيا

m.emsaad@uot.edu.ly
malekfarhat06@gmail.com

DOI: https://10.5281/zenodo.18114791

الملخص: لا تزال الشبكات المحلية LAN عرضةً للهجمات التي تعتمد على البروتوكولات، وتستغل نقاط الضعف في خدمات الشبكة الأساسية. ومن أكثر أنواع هذه الهجمات شيوعًا: حرمان الموارد من بروتوكول DHCP ، وانتحال بروتوكول ARP، والانتقال بين عناوين الشبكة المحلية الافتراضية VLAN، والتي قد تُعرّض سرية الشبكة وسلامتها وتوافرها للخطر الشديد. هذه الدراسة تبحث في فعالية اختبار الاختراق لتحديد هذه الثغرات الأمنية والتخفيف من آثارها في بيئات الشبكات المحلية. تم تصميم شبكة محاكاة باستخدام برنامج GNS3، ونُفذت هجمات مُحكمة باستخدام نظام Kali Linux ومجموعة أدوات Yersinia لتقييم مرونة الشبكة. بناءً على نتائج اختبار الاختراق، تم تحديد الثغرات الأمنية والتخفيف من آثارها باستخدام آلية أمنية واحدة، وهي أمان المنافذ. تُظهر النتائج التجريبية أن تطبيق أمان المنافذ قد قلل بشكل كبير من عدد الهجمات الناجحة وحسّن أمان الشبكة بشكل عام. تُبرز النتائج أهمية اختبار الاختراق كنهج عملي لتعزيز أمن الشبكات المحلية، وتقدم توصيات فعّالة من حيث التكلفة تناسب المؤسسات الصغيرة والمتوسطة.

الكلمات المفتاحية: الهجمات السيبرانية، اختبار الاختراق، حرمان DHCP، انتحال ARP، تغيير VLAN، أمن المنافذ.