JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 06 Issue 02
2024

Research Article
https://doi.org/10.56979/602/2024

Enhancing LAN Security by Mitigating Credential Threats via HTTP Packet Analysis with Wireshark

Altaf Hussain[1], Aamir Hussain[1*], Salman Qadri[1], Abdul Razzaq[1], Hira Nazir[1], and Muhammad Sami Ullah[2]

[1]Institute of Computing, Muhammad Nawaz Sharif University of Agriculture Multan, Pakistan.
[2] Govt. Graduate College of Commerce, Multan, Pakistan.
*Corresponding Author: Aamir Hussain. Email: aamir.hussain@mnsuam.edu.pk

Received: November 09, 2023 **Accepted:** February 28, 2024 **Published:** March 01, 2024

Abstract: The world is connected digitally and the security of Local Area Networks has been dangerous increasingly. A process that is especially designed to secure networks from different ouside attacks is known as Cybersecurity. In this article, a Local Area Network threat scenario is discovered especially concentrating on the extraction of credentials by capturing the Hypertext Transfer Protocol packets. Most of the time, Local Area Network can be said a secure, but sometimes itcan have many vulnerablities to cybersecurity threats. An attacker can be connected with Local Area Network and using packets capturing and network anlysing tool wireshark; they can exploit the Hypertext Transfer Protocol vulnerabilities to obtain login credentials. Attackers have motives to get specific credentials, they perform actions to get IP addresses, emal addresses being used in communication and financial details, by network trffic examination. Differenet protocols such as Hypertext Transfer Protocol, Address Resolution Protocol, and Transmission Control Protocol are can be captured and analyzed by this tool. To get filtered packets, Wireshark provides the best filtering selections and interpret into packets. For the security of Local Area Network, implementation of various security approaches including encryption of data and protocols, Firewall, IDS/IPS implementation, network segmentation, ethernet cables usage, use of Hypertext Transfer Protocol Secure and Multifactor authentication is deployed. Network traffic should be monitored, apply port security, and allow only registered Media Access Control in Access Point. The proposed solution enhanced the security of the Local Area Network and mitigated the cybersecurity threats. Network and connected devices monitoring regularly and activity of traffic packet-capturing tools can make the Local Area Network more secure.

Keywords: Cybersecurity; Wireshark; Vulnerabilities; HTTP; LAN-based; Capture data; Credentials; Mitigation.

1. Introduction

Security of Local Area Networks has been a very serious issue in the digital world day by day. For the protection of all digital devices from different threats, a Cyber security process is designed [1]. A wired network in which different users are communicating is known Local Area Network (LAN). LAN is the backbone of the organizational operations that facilitates communication between users [13]. In LAN many security threats can be dangerous for the network. Hypertext Transfer Protocol that works on port 80 is vulnerable in LAN [2]. For capturing the HTTP packets, a packet-capturing tool named Wireshark is used. This is a powerful packet-capturing tool that plays an important role in unveiling network difficulties and offers insight into the exploitation of HTTP packets for credentials access [12]. Wireshark has ability to capture and then analyze many protocols such as HTTP, ARP, TCP, DNS etc. [3].

1.1. Local Area Network

LAN is the type of computer network where many devices are connected within a physical limited area including Office building, home, or school is called Local Area Network. An organization has LAN as its backbone for operations and most resources including printers, files are shared, and internet connectivity is provided [14]. LANs are helpful for education and critical to ensure security against threats. LANs are vulnerable to cyber security threats such as data breaches and unauthorized access. Using the network traffic capturing and analysis tool, vulnerabilities of network can be found and mitigated [3]. LAN figure is given as figure 1.

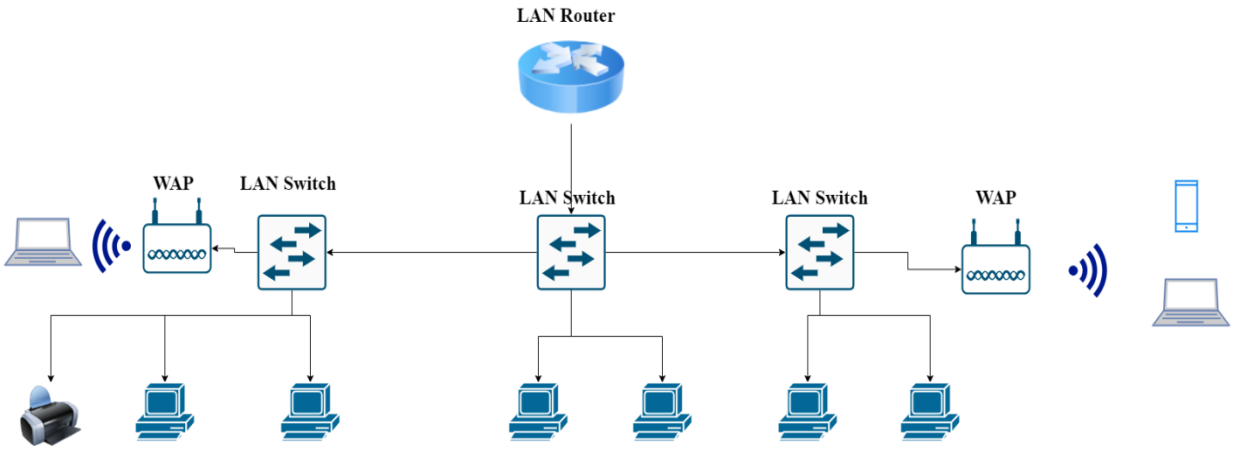

Figure 1. Local Area Network Design

1.2. Wireshark Tool

Wireshark is a network protocol analyzer tool available as open source and used to examine and understand network traffic using protocols within a network. Being a useful tool, it allows users to capture the traffic, analyse and interpret the packets to valued insight into network behavior and vulnerabilities presented in that network [4]. A LAN defense is used to recognize different threats which can be mitigated. To address the security weak points, protocol vulnerabilities, and traffic behavior, this tool is used [3].

1.3. Network Protocols

In LAN, there are many protocols used for effective communication and data exchange. Using Wireshark, fundamental protocols can be captured. Transmission Control Protocol (TCP) is a connection-oriented protocol and can be used for the establishment of a connection between two devices [5]. Internet Protocol (IP) is used for the addressing and packet routing within the network. It provides the foundation for the internet so devices can communicate by unique addresses for each device. Hypertext Transfer Protocol (HTTP) is a protocol that is used to transmit hypermedia documents between devices. It provides communication on the World Wide Web (WWW) and allows browsers to display webpages [6]. File Transfer Protocol (FTP) is used for file transfer from server to client over the network. Simple Mail Transfer Protocol (SMTP) is used for email sending across the network. Domain Name System (DNS) is used to change domains that are human-readable into IP addresses [4].

2. Related Work

The wireshark role was emphasized as a network protocol analyzer that addresses an important need for an administrator to find and overcome potential threats in the network. It provided the ability of Wireshark to inspect and analyze network traffic and provide the OSI model traffic flow in the network. It

reported different LAN attacks including MAC flooding, ARP poisoning, DNS spoofing, and DOS attacks. It also demonstrated how Wireshark can detect and address security challenges [3].

Different network security threats and their mitigation methods were reported in detail. For the protection of network threats, different security methods including strong passwords, security policies enforcement, use of Firewalls, and monitoring the network activities were proposed [7].

The dataset role was emphasized in the evaluation of the efficacy of deep packet inspection (DPI) for cyber security. Due to the complexity of cyber threats, different researchers emphasized the need for different datasets to cover a wide range. Datasets were taken from cybersecurity organizations to find harmful and harmless network actions. Overall DPI work is elaborated to improve cybersecurity in real-time [1].

In accessing network security, current research, methodologies, and tools are reported well in the systemic review. Gaps in present work and future suggestions to enhance the penetration testing practices were provided [14]. A complete guide to new researchers for the network security assessment was provided for further investigation and exploitation of network vulnerabilities [8].

The packet sniffer's role played in the network traffic analysis was described with a concise overview. Using packet sniffing tools, different cybersecurity threats such as bottlenecks, potential security threats, and service disruption in computer networks were highlighted [16]. The ability of packet sniffers to monitor, analyze, and map network traffic is succinctly outlined here. Packet sniffers have functionalities to detect and then mitigate different local area attacks to enhance the security and resilience of the network [9].

Protection of IoT-based smart homes from cyber threats was reported. Some threats including unauthorized access to someone's data, vulnerabilities of the network and data breaches in smart homes were highlighted. For the protection of home network from various kinds of attacks, many security mechanisms including encryption method, authentication, network monitoring and updating the system were deployed [10].

Some key challenges for the security of Wireless Local Area Network (WLAN) were described. Various loopholes like way to unauthorized access and lack of encryption method were highlighted to focus on the implementation of wireless technologies [15]. Bes security mechanisms including encryption of data using protocols, strong authentication with MFA, and deployment od intrusion detection systems, to mitigate these threats highlighted the importance of strong security implementation. The major aim was to provide short insights into the WLAN security for the confidentiality and integrity of wireless communication could be ensured [11].

In our research, the main objective is to capture packets and explore them using a packet sniffer such as Wireshark, and then go insight into HTTP packets for taking credentials. As finding the vulnerability of HTTP, we have to capture HTTP Post packets and can obtain login credentials including usernames and passwords of the users communicating on the network. After identification of various vulnerabilities, our main aim is to apply different security approaches for the protection of our Local Area Network and its traffic. Our research aims to enhance LAN security through implementation of security mechanisms.

3. Material and Methodology

By adopting all critcal steps, we should find the HTTP vulnerabilities, packet capturing, interpret into packets, obtain credentials, and then to make it secure, implement some security measurements. Being the security analyst, we have to explore vulnerabilities in our Local Area Network (LAN). Using Wireshark which is a powerful tool to capture and analyze the traffic, we explored insight into traffic and protocols.

3.1. Get Access to LAN

Using different techniques such as password dictionary attacks having SSID of WLAN and using Ethernet connectivity, we got access to Local Area Network (LAN). We opened our device CMD and found the IP address using the command "config/all". We obtained the IP address and default gateway of the network. We scanned the network ID into the network scanner tool and found that many users were working on the LAN. We got their IPs, OS, and open ports by applying "nmap" commands.

3.2. Capture LAN Traffic

We started the Wireshark application on our device and used an appropriate network interface to get network traffic. By having a Wi-Fi connection we clicked on the Wi-Fi interface module and waited for some time to capture a lot of network traffic. We got packets with different IPs, protocols, and services. We waited and explored network traffic continuously as shown in Figure 2. As users on LAN were communicating, we monitored their activities.

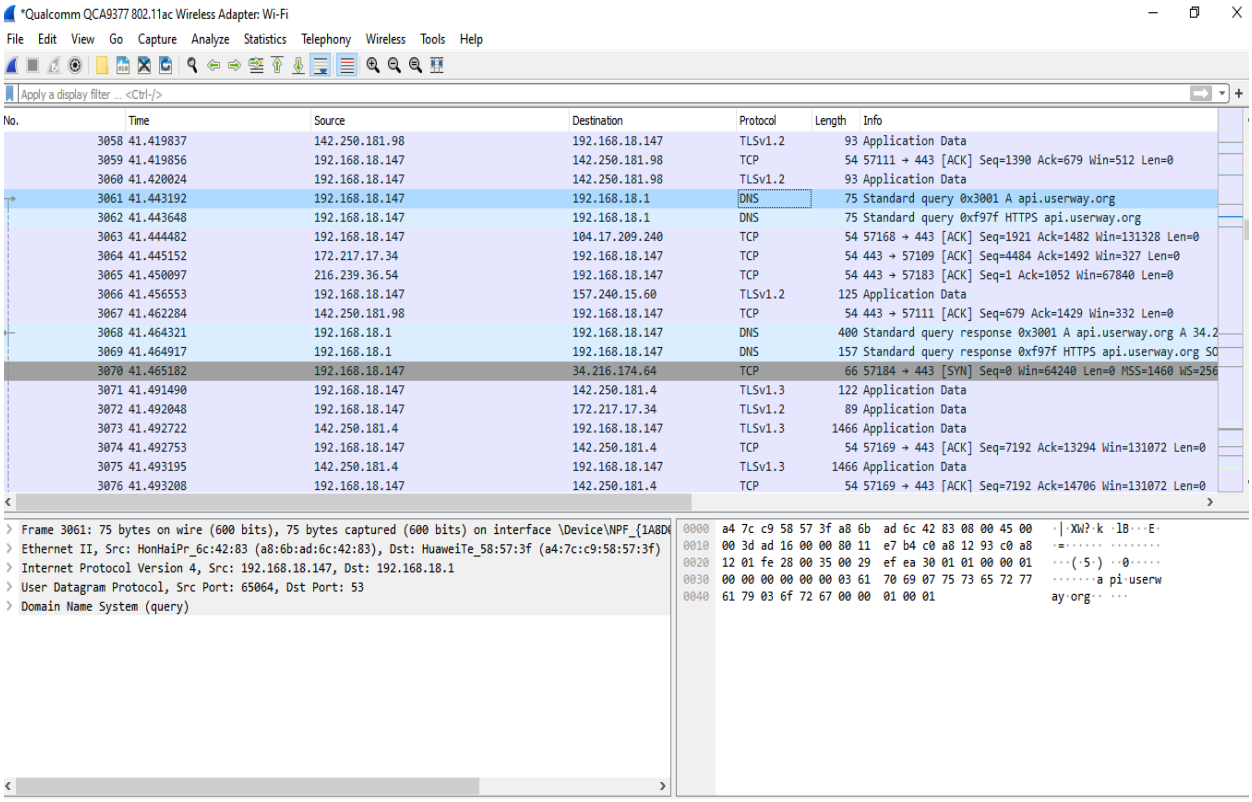

Figure 2. Wireshark Packets Capturing Results

3.3. Capture HTTP Packets

We got a lot of packets but we wanted to find the http services. Using filter "http" we obtained traffic with only HTTP GET and POST packets. We observed that there were some POST packets given in captured traffic. In this step, we got the Packet number, Time, Source and Destination IP address, Protocol, and information regarding them as shown in Figure 3.

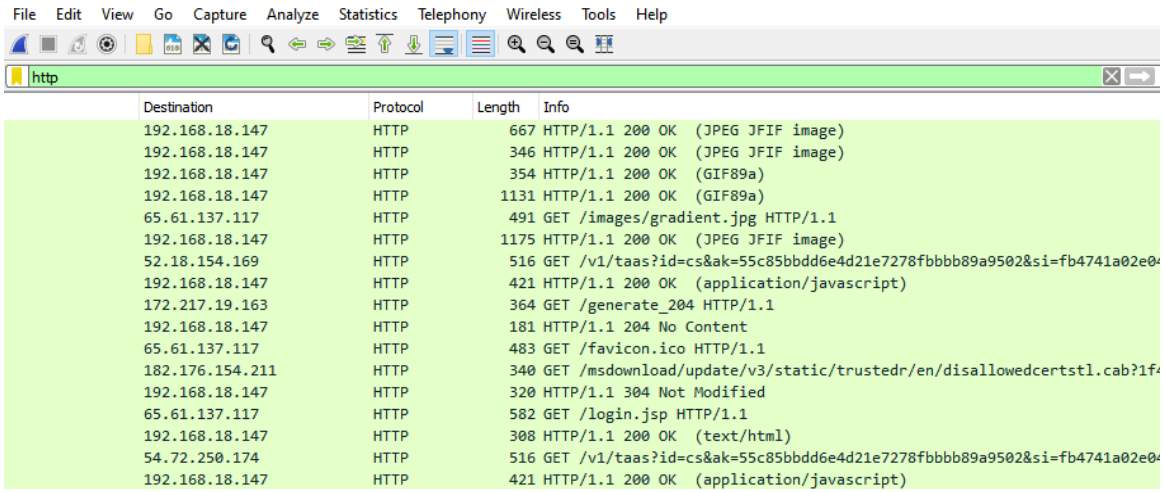

Figure 3. HTTP Packets Captured

3.4. Analyze HTTP Packets

To analyze the network traffic, in the filter, we applied "http.method == "POST"". We got some packets with the HTTP post. Their IPs, protocols, and information were given there. We analyzed Post HTTP packets to get their sender and receiver IP addresses. We explored the port numbers associated with the sender and receiver. Window size, packet size, header, and other related information were explored.

3.5. Identify Credentials Threats

In this section, we explored the part as a hypertext transfer protocol in Wireshark. We obtained information regarding the URL where credentials were used, credentials including username and password. We got that they were given in plaintext and read by humans easily. We got credentials used by users in LAN and they got logged in and performed their activities. That was the actual HTTP vulnerability captured by Wireshark as shown in Figure 4.

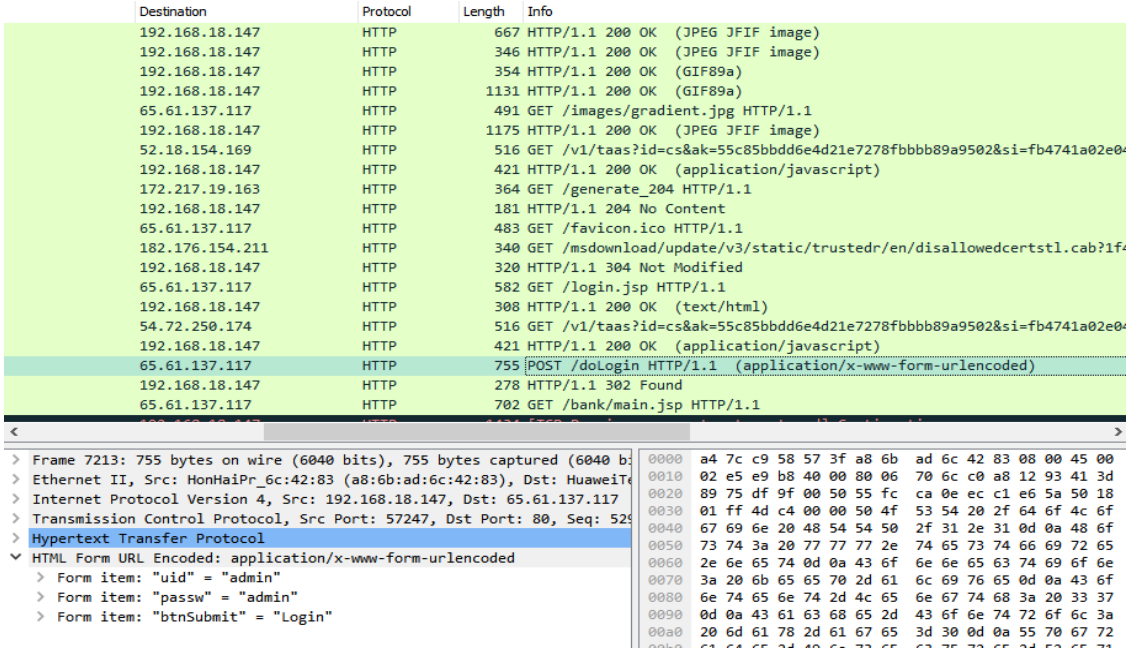

Figure 4. Credentials Obtaining in HTTP Packets

3.6. Mitigate Credentials Threats

Hypertext Transfer Protocol is used for the plaintext information and does not use any encryption method. We aimed to mitigate the credentials; we applied encryption in login and used HTTPS instead of HTTP. Different mechanisms such as applying multifactor authentication, encryption, physical security of LAN, and firewall rules allow only permitted users to be connected.

3.7. Monitor Network Activity

After the implementation of security measurements, we monitored our LAN regularly. We also used network scanning tools to scan networks and open ports which are vulnerable. We applied again security mechanisms to close the vulnerable ports on every device on LAN. Using Wireshark, capture traffic to check different protocols and their vulnerabilities, and working, we monitor any unauthorized access in the network. Methodology steps are given in figure 5.

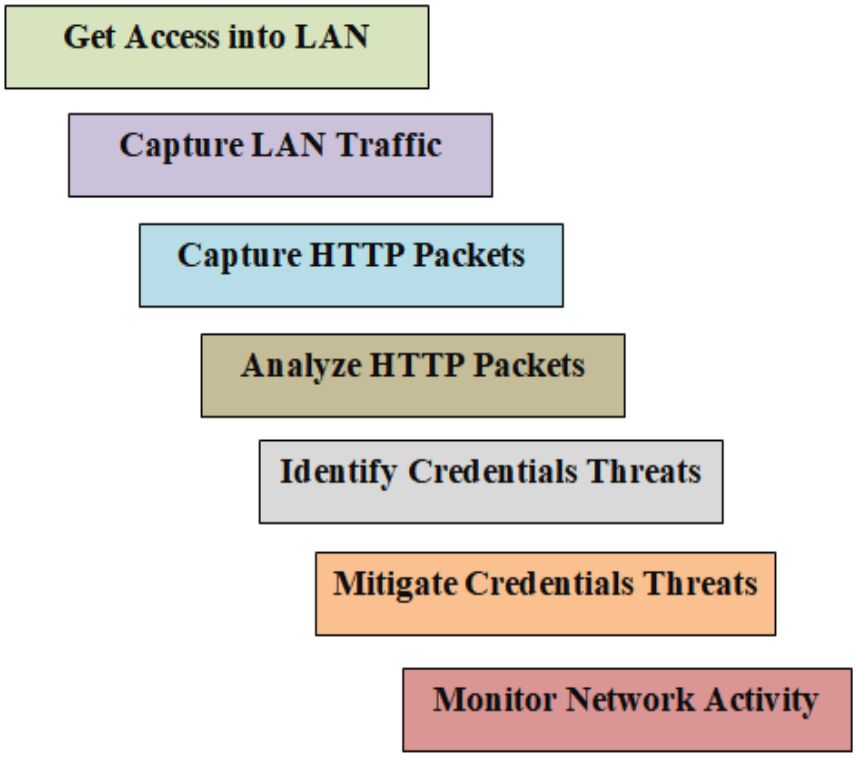

Figure 5. Methodology Steps to Find HTTP Vulnerability

4. Results

We applied Wireshark and captured network traffic, we analyzed the HTTP vulnerability. HTTP is vulnerable and its login credentials can be explored by its packet interpretation. In LAN network access any unauthorized person can provide access to the network and using any network scanning tool, an attacker can scan and then sniff packets using sniffers such as Wireshark. In our LAN, we explored HTTP vulnerability, and its Post packet and then got login credentials used by any other user in the network. Results provide information on the effectiveness of network sniffer "Wireshark" and analyzing network traffic, vulnerabilities, and attacks to obtain credentials using HTTP post Packets as shown in Table 1 and figure 6. Implementation of high-security measurements makes LAN well-secured and enhances organizational security.

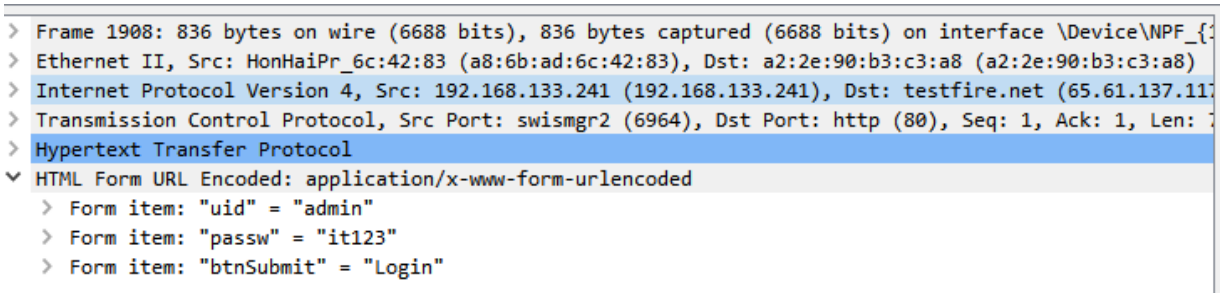

Figure 6. Login Credentials

Table 1. HTTP Packets Captured Results

Src. IP	Dst. IP	Protocol	Username	Password
192.168.18.147	65.61.18.117	HTTP	admin	admin
192.168.133.241	65.61.18.117	HTTP	admin	it123
192.168.133.243	65.61.18.117	HTTP	itian	123itian

5. Discussion

LAN is the backbone of the operations of any organization. Its security is the main concern because it contains very confidential information. Due to a lack of understanding and awareness of network security, mostly LANs can be compromised. It is well known that HTTP is vulnerable, but still, many organizations are using HTTP web servers and domains so the chances of their compromising are increased. Unauthorized access can lead to stealing information or destroying organizational operations. So security measurements are necessary to be implemented with secure socket layer (SSL) certificates. Regular monitoring of the network is necessary to make LAN secure.

6. Conclusion

This study demonstrated that Wireshark is a powerful tool used to capture, analyze, and interpret packets of network traffic. The use of network scanning and sniffing tools like Wireshark is to analyze HTTP packets and explore credentials on LAN. HTTP packets contained plaintext credentials that were used by LAN users. LAN is important for any organization that keeps different types of confidential information, so its security is very crucial. Applying security techniques such as physical security, use of Firewall, use of HTTPS, encryption, multifactor authentication, and monitoring enhanced the LAN security. Regular updating of the passwords is also the best technique to make the login secure which needs OTP encrypted in network traffic to secure the LANs.

References

1. S. K. Shandilya, C. Ganguli, I. Izonin, and P. A. K. Nagar, “Cyber attack evaluation dataset for deep packet inspection and analysis,” Data Br., vol. 46, p. 108771, 2023, doi: 10.1016/j.dib.2022.108771.
2. A. Siswanto, A. Syukur, E. A. Kadir, and Suratin, “Network traffic monitoring and analysis using packet sniffer,” Proc. - 2019 Int. Conf. Adv. Commun. Technol. Networking, CommNet 2019, no. April, 2019, doi: 10.1109/COMMNET.2019.8742369.
3. H. Iqbal and S. Naaz, “Wireshark as a Tool for Detection of Various LAN Attacks,” Int. J. Comput. Sci. Eng., vol. 7, no. 5, pp. 833–837, 2019, doi: 10.26438/ijcse/v7i5.833837.
4. U. Banerjee, A. Vashishtha, and M. Saxena, “Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection,” Int. J. Comput. Appl., vol. 6, no. 7, pp. 1–5, 2010, doi: 10.5120/1092-1427.
5. A. Varanasi and P. Swathi, "Comparative Study of Packet Sniffing Tools for HTTP Network Monitoring and Analyzing," vol. 6, no. 12, pp. 406–409, 2016.
6. M. Kushnir, O. Favre, M. Rennhard, D. Esposito, and V. Zahnd, "Automated Black-Box Detection of HTTP GET Request-based Access Control Vulnerabilities in Web Applications," Int. Conf. Inf. Syst. Secur. Priv., no. Icissp, pp. 204–216, 2021, doi: 10.5220/0010300102040216.
7. L. F. Sikos, “Packet analysis for network forensics: A comprehensive survey,” Forensic Sci. Int. Digit. Investig., vol. 32, p. 200892, 2020, doi: 10.1016/j.fsidi.2019.200892.
8. M. Alhamed and M. M. H. Rahman, “A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions,” Appl. Sci., vol. 13, no. 12, 2023, doi: 10.3390/app13126986.
9. J. Biswas and A. Ashutosh, "An Insight into Network Traffic Analysis using Packet Sniffer," Int. J. Comput. Appl., vol. 94, no. 11, pp. 39–44, 2014, doi: 10.5120/16391-5975.
10. A. Hussain, A. Hussain, S. Marjan, M. Baryalai, Z. Zaland, and A. Wahid, “Cyber Security Challenges and Attacks and Countermeasures for IoT-Based Smart Home,” no. 12, pp. 166–172.
11. M. Waliullah and D. Gan, "Wireless LAN Security Threats & Vulnerabilities: A Literature Review," Int. J. Adv. Comput. Sci. Appl., vol. 5, no. 1, pp. 176–183, 2014.
12. R. Das and G. Tuna, “Packet tracing and analysis of network cameras with Wireshark,” 2017 5th Int. Symp. Digit. Forensic Secur. ISDFS 2017, no. April 2017, 2017, doi: 10.1109/ISDFS.2017.7916510.
13. E. Golden and J. W. Coffey, "A Tool to automate the generation of wireshark dissectors for a proprietary communication protocol," 6th Int. Multi-Conference Complexity, Informatics Cybern. IMCIC 2015 6th Int. Conf. Soc. Inf. Technol. ICSIT 2015 - Proc., vol. 1, pp. 53–56, 2015.
14. M. A. Qadeer, M. Zahid, A. Iqbal, and M. R. Siddiqui, “Network traffic analysis and intrusion detection using packet sniffer,” 2nd Int. Conf. Commun. Softw. Networks, ICCSN 2010, pp. 313–317, 2010, doi: 10.1109/ICCSN.2010.104.
15. S. Pavithirakini, D. D. M. M. Bandara, C. N. Gunawardhana, K. K. S. Perera, B. G. M. M. Abeyrathne, and D. Dhammearatchi, “Improve the Capabilities of Wireshark as a tool for Intrusion Detection in DOS Attacks,” Int. J. Sci. Res. Publ., vol. 6, no. 4, p. 378, 2016. Available: www.ijsrp.org
16. J. Sulicdio, T. U. Kalsum, and Y. Arliando, “Comparative Analysis of Wireshark and Windump Software in Network Security Monitoring,” J. Media Comput. Sci., vol. 1, no. 1, p. 1, 2022.