Journal of Computer Networks, Architecture and High Performance Computing
Volume xx, Number xx, month Year
https://doi.org/10.47709/cnahpc.v4i1.1345

Submitted : Jan 20, 2022
Accepted : Jan 25, 2022
Published : Jan 25, 2022

Implementation of Wireshark Application in Data Security Analysis on LMS Website

I Kadek Noppi Adi Jaya[1)*], Ida Ayu Utari Dewi[2)], Gede Surya Mahendra[3)]
[1)2)]Universitas Hindu Indonesia, Indonesia, [3)]STMIK STIKOM Indonesia, Indonesia
[1)]iknadijaya@unhi.ac.id, [2)]utaridewi@unhi.ac.id, [3)]gede.mahendra@stiki-indonesia.ac.id

ABSTRACT

Data security issues are an important aspect of data and information communication over networks. In addition, it is also necessary to look at the security side of the software. In addition to software, computers have an internet protocol in the form of HTTP which is commonly used to access websites. On the LMS website, students have access to lecture materials, discussion forums with lecturers and access to assignments given by lecturers. Wireshark is used to analyze network protocols, can log all packets going through and display detailed data. The purpose of this study is to use a Wireshark application to sniff LMS and pinpoint vulnerabilities in the system. The results of the sniffing process carried out using Wireshark on an LMS that uses the HTTP protocol clearly indicate the absence of encryption and expose the risk of vulnerabilities to the system. Recommendations given to LMS are the use of HTTPS protocol, implementation of Multi Factor Authentication, website log monitoring and password management. Recommended password management are periodic password changes, standardization policies for the use of characters in passwords and password hashing. It is hoped that when the recommendations are implemented it will improve security on the LMS website and reduce risks in data communications

Keywords: LMS, Security, Sniffing, Website, Wireshark

INTRODUCTION

Data security issues are an important aspect of data and information communication over networks. Advances in the field of computer networks and the concept of open systems, making it easier for people to access the network. This can result in the process of sending data at risk of being unsafe and can be used by other people or parties who are not responsible for retrieving data or information in the middle of the road (Huzaeni, Gunawan, Purnomo, Yanti, & Krisdayanti, 2021). There is also a risk of data theft on the network or hackers shutting down network resources (Nitra & Ryansyah, 2019).

In addition to the importance of security in the circulation of data and information in the network, it is also necessary to look at the security of the software. In carrying out its operation, the computer has supporting software which runs on top of the operating system and plays a very important role in performing the tasks performed by the users. With the help of software, the computer can execute commands that help the user's work. However, not all software can support and accelerate human work, and there are several types of software that can cause damage or harm other users, such as malware which is dominated by 3 categories of malware, first the malware category itself (44%) followed by Adware (38%) and the last one is Trojan (18%) (Manoppo, Lumenta, & Karouw, 2020).

In addition to software that runs on a computer operating system, it also has an internet protocol in the form of HTTP which is commonly used to access websites or web-based platforms. This technology will never erode over time, because the site can be accessed quickly from almost any technology device, such as smartphones, notebooks, tablets, and others. Because of this convenience, more and more security holes appear, and it is not uncommon for internet network users to become victims due to a lack of understanding of website security protocols. The stolen data is usually the username and password of the victim's account, which is used for malicious purposes. In previous studies, several studies have been conducted regarding the use of Wireshark to determine network security (Abdillah, Yudhana, & Fadil, 2020; Luthfansa & Rosiani, 2021; Malek & Amran, 2021).

Learning Management System (LMS) is an information technology system designed to manage and support the learning process, distribute lecture materials, and enable collaboration between lecturers and students (Fitriani, 2020).

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume xx, Number xx, month Year
https://doi.org/10.47709/cnahpc.v4i1.1345

Submitted : Jan 20, 2022
Accepted : Jan 25, 2022
Published : Jan 25, 2022

At LMS, students have access to lecture materials provided, discussion forums with lecturers through forums, chats, and access to assignments given by lecturers. Instructors are also encouraged to be creative with learning materials through learning videos that can be uploaded to the LMS. LMS contributes in terms of utilization. The flexibility of the learning management system allows instructors and students to access the LMS anytime, anywhere from a variety of devices.

Based on the considerations that have been described previously, the condition of data security in the LMS is a vital concern. The urgency of this research is that if it is not carried out immediately, the LMS website will expose a lot of sensitive data from its users so that it will pose a high risk to data security. There will be vulnerabilities to campus data security, making it easier for data security criminals such as hackers to steal users' personal data to damage internal systems. So that research on the implementation of the Wireshark application in data security analysis on the LMS website needs to be carried out and the recommendations given from the results of this study need to be considered.

LITERATURE REVIEW

Learning Management System (LMS) is a technical term specifically used to manage and facilitate the entire online learning process (Rakhmawati, Mardliyah, Fitri, Darni, & Laksono, 2021). LMS, also known as Course Management System (CMS) or Virtual Learning Environment (VLE), is a software application used by educators at universities/colleges and schools as internet-based online learning media (e-learning). By using LMS, Lecturers/Teachers/Instructors can manage programs/classes and exchange information with students. In addition, access to learning materials that occur within a predetermined period of time (Putri, 2018). The functions provided by LMS to educational institutions are managing user access rights, managing courses, managing teaching materials (resources), managing activities, managing grades, displaying grades and transcripts, and managing grades. visualization of e-learning so that it can be accessed using a web browser. Examples of LMS platforms include Google Classroom, Canvas, Moodle, Edmodo, Schoology, and others (Yana & Adam, 2019).

Hypertext Transfer Protocol (HTTP) is an application network protocol used to distribute information between server computers and client computers. The server is a place full of all kinds of information, and its main task is to provide one or more services to the clients connected to it (Riswandi, Kasim, & Muh. Fajri Raharjo, 2020). A client is a web browser that can access, receive and display content through a browser. HTTP is the most widely used protocol and there are many resources available on the Internet (Alexander, Salkiawat, & Warta, 2021).

In the HTTP protocol, there is no guarantee that the data between the client and the server is secure. This causes many criminal problems, such as leakage of personal data entered on the web using the HTTP protocol. Basically, every communication protocol between client and server always uses the HTTP concept. However, if you want to implement a more secure protocol, you will need an SSL (Secure Sockets Layer) certificate. Web pages that use the HTTP protocol will be more difficult to access, or even fail to open and be redirected to another page.

Sniffing is a form of cybercrime where the perpetrator steals other people's usernames and passwords intentionally or unintentionally (Ihsana & Maslan, 2020). Sniffing is the process of getting data packets sent over a computer network. Sniffing can be used to monitor and capture all traffic occurring within it, regardless of where and to whom packets are sent. A negative side effect of sniffing is the ability to see confidential information, such as usernames and passwords, from other people connected to the network. The role of a good network sniffing is to analyze packets that pass through the network so that the network is more optimal, analyze whether the data affects network performance, and find out whether outside parties have penetrated the network so as to increase network security.

Wireshark is a program to analyze network protocols, can record all packets that go through and display detailed data, Wireshark is mainly used to track the network management of a company or institution so that it can ensure that the network is functioning properly and can track what is happening on the network (Prayitno, 2019; Susianto & Rachmawati, 2018). Wireshark is also known as network packet analyzer; its function is to display all packet information and capture packets sent and received. Wireshark was formerly known as Ethereum, which was developed by Gerald Combs in 1988 (Iqbal & Naaz, 2019). The network packet analyzer can be used to monitor a variety of networks, both wired and wireless. With this Wireshark, administrators will find it easier to monitor the network because the data captured in Wireshark can be saved and reopened for analysis. In Wireshark data can be captured wired or wirelessly. Data can be read from various types of networks, including Ethernet, IEEE 802.11 or Point-to-Point Protocol (PPP) (Maulana, Walidainy, Irhamsyah, Fathurrahman, & Bintang, 2021).

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume xx, Number xx, month Year
https://doi.org/10.47709/cnahpc.v4i1.1345

Submitted : Jan 20, 2022
Accepted : Jan 25, 2022
Published : Jan 25, 2022

METHOD

In this study, the authors use data collected by capturing packets using the Wireshark application. The data is accessed from the LMS of the Universitas Hindu Indonesia, namely lms.unhi.ac.id, using the HTTP protocol. Figure 1 shows the research flow on the implementation of the Wireshark application in data security analysis on the LMS website carried out at the LMS of the Universitas Hindu Indonesia which is accessed at lms.unhi.ac.id. The first process that must be done is to activate the Wireshark application by selecting a wifi network, then we must visit the website address that we will visit as an example after waiting for Wireshark to retrieve packets through the browser. Turn off or stop packet capture in Wireshark while packets are being fetched to make it easier to analyze the packets. Filter using HTTP, then search for packages via the posting method and analyze the contents of those packages.

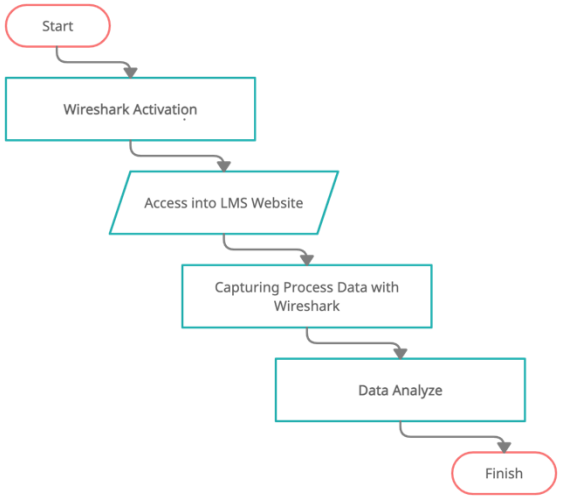

Fig. 1 Research Flowchart

RESULT

The result of implementing the Wireshark application in data security analysis on the LMS website is to first analyze the website using HTTP, and use Wireshark for sniffing to get the username and password. The specific steps are as follows. The first step is run the Wireshark application. In this study, the authors use data collected by capturing packets using the Wireshark application. The data is accessed from the LMS of the Universitas Hindu Indonesia, namely lms.unhi.ac.id using the HTTP protocol. The version of the Wireshark application used is version 3.6.1 on Windows. The following is an initial view of the Wireshark version 3.6.1. application, which is shown in Figure 2. The ping process on the LMS page is shown in Figure 3.

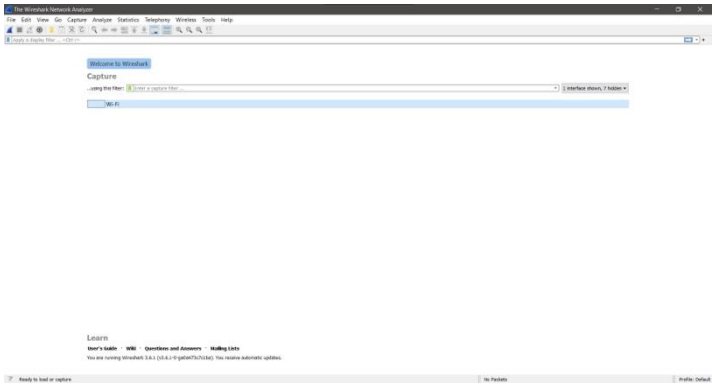

Fig 2. Initial Display of Wireshark 3.6.1

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume xx, Number xx, month Year
https://doi.org/10.47709/cnahpc.v4i1.1345

Submitted : Jan 20, 2022
Accepted : Jan 25, 2022
Published : Jan 25, 2022

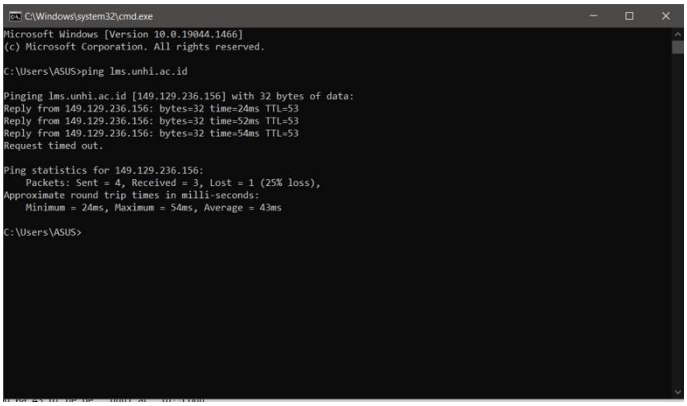

Fig 3. Ping Display on LMS Using Command Prompt

Second step is specifying the HTTP address. Here we use the address lms.unhi.ac.id/login/index.php for the sniffing process to get the username and password. The appearance of the LMS website page is shown in Figure 4 and the “not secure” view is shown in Figure 5. The “not secure” view is obtained because the LMS website still uses the HTTP protocol. This condition indicates insecurity in accessing the LMS website. In order to be more complete in knowing what conditions occur behind the "not secure" condition, one of them can be proven by using Wireshark in sniffing action on the LMS website.

Fig 4. LMS Website Page Display

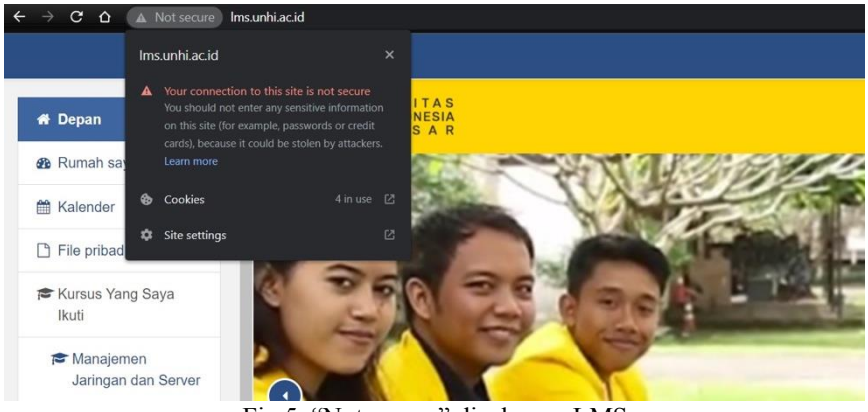

Fig 5. “Not secure” display on LMS

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume xx, Number xx, month Year
https://doi.org/10.47709/cnahpc.v4i1.1345

Submitted : Jan 20, 2022
Accepted : Jan 25, 2022
Published : Jan 25, 2022

Third step is capture data using Wireshark. After activating the Wireshark application and specifying LMS access, the Wireshark application will capture incoming and outgoing data. The following is the initial view of the data retrieval page (sniffing) on the Wireshark application which is shown in Figure 6, while the display of the data retrieval (sniffing) page using the Wireshark application is shown in Figure 7.

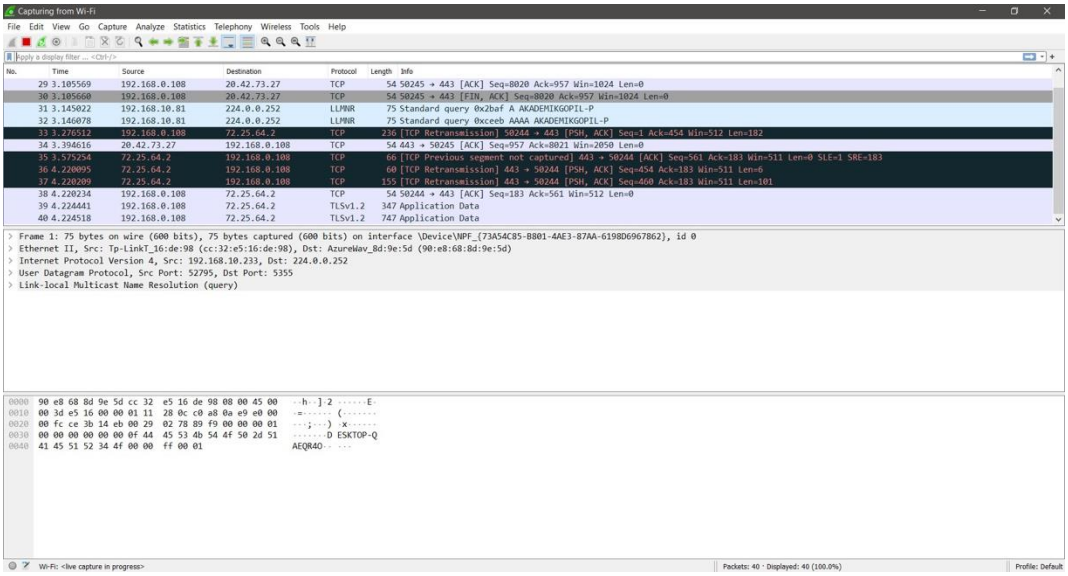

Fig 6. Initial View of the Data Capture (Sniffing) Page Using Wireshark

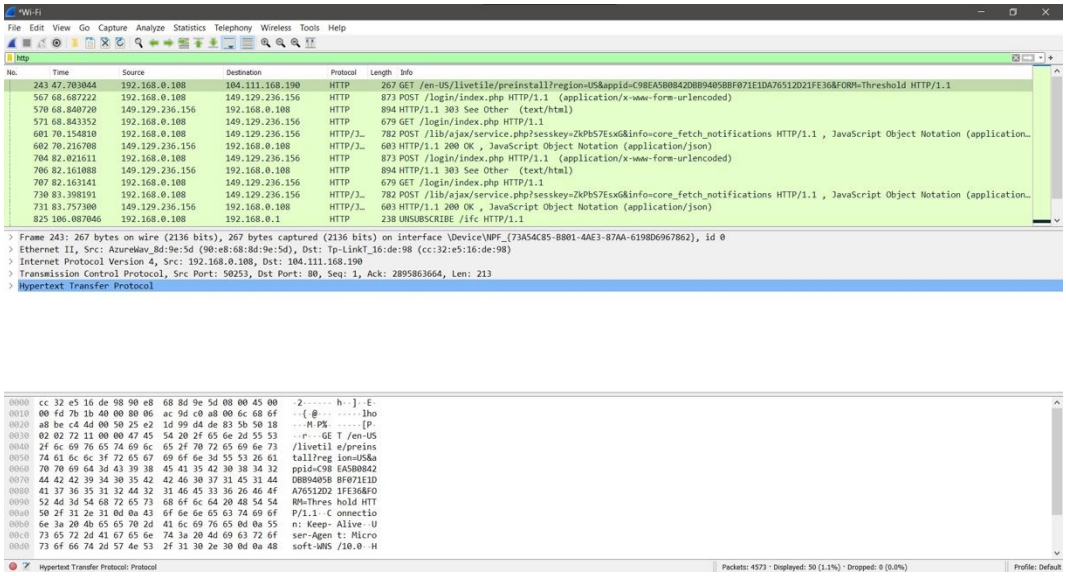

Fig 7. Process Display of the Capture Data (Sniffing) Page Using Wireshark

Fourth step is testing. After the sniffing process using the Wireshark application is active, then access the LMS website and enter the username and password on the website. The display of the username and password page on the LMS is shown in Figure 8, and the dashboard page display during successful login is shown in Figure 9.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume xx, Number xx, month Year
https://doi.org/10.47709/cnahpc.v4i1.1345

Submitted : Jan 20, 2022
Accepted : Jan 25, 2022
Published : Jan 25, 2022

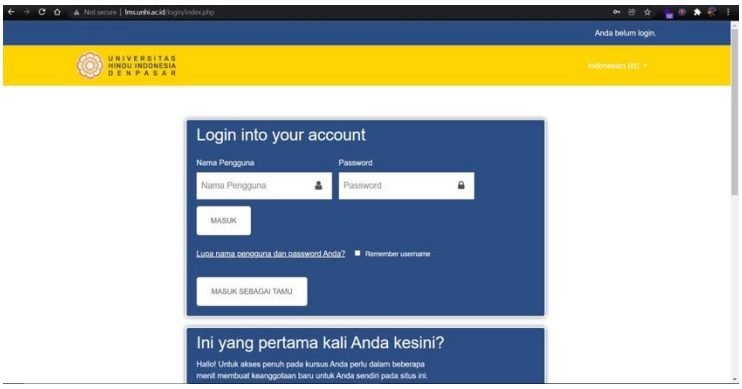

Fig 8. Username and Password Page Display on LMS

Fig 9. Dashboard Page Display When Successfully Login to LMS

Fifth step is stop the data collection process. Return to the Wireshark application and "stop capture" on the running process. Type the HTTP command in the filter and select POST in the info section. After data collection complete, we need to search the information. In the POST data there is information such as the IP address 192.168.0.108 at the source and 149.129.236.156 at the destination, then in HTTP there is various information then select the HTML form to find out the username and password that was entered earlier. The display of POST packet analysis on the login process can be seen in Figure 10.

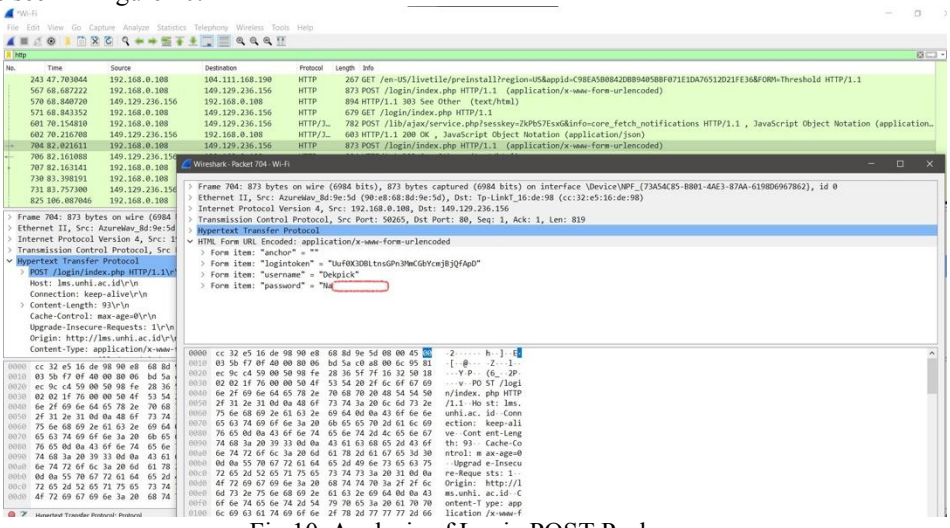

Fig 10. Analysis of Login POST Packages

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume xx, Number xx, month Year
https://doi.org/10.47709/cnahpc.v4i1.1345

Submitted : Jan 20, 2022
Accepted : Jan 25, 2022
Published : Jan 25, 2022

Last step is sniff results. Sniffing usernames and passwords using the Wireshark app has worked. With the capture results that are analyzed through the network on the selected network, the username and password on the POST data packet can be known. The HTML page display that displays the username and password displayed on encryption is shown in Figure 11.

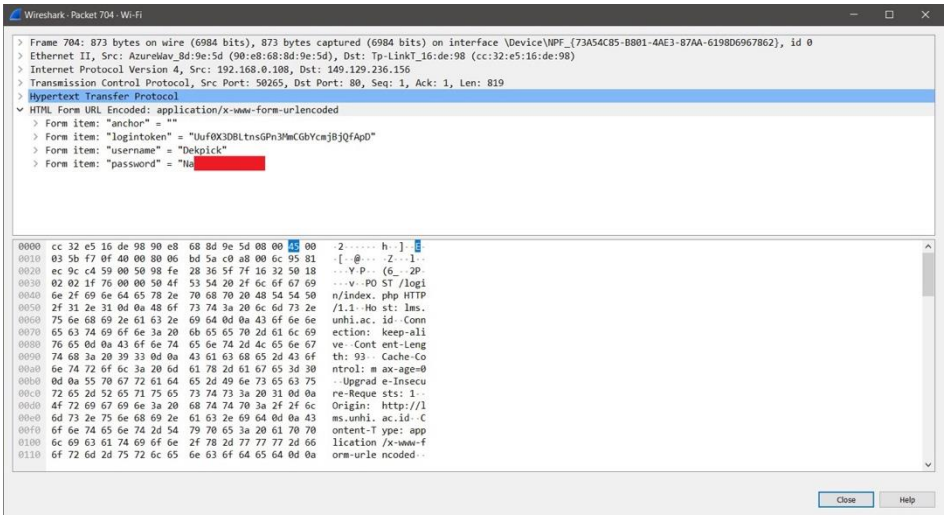

Fig 11. HTML Page Display Showing Username and Password Visible Without Encryption.

DISCUSSIONS

The results show that the Wireshark application can be used to find weaknesses in the LMS owned by the Hindu University of Indonesia. The sniffing process carried out using Wireshark at the address lms.unhi.ac.id which uses the HTTP protocol clearly indicates the absence of encryption and creates a vulnerability to user access. To improve security and prevent data and information leakage at the LMS belonging to the Hindu University of Indonesia, there are several recommendations as follows. Implementing the HTTPS protocol, which aims to improve the security of communication in the network between users and web servers with data encryption so as to prevent leakage of confidential information such as usernames, passwords or other sensitive information. Implemented Multi Factor Authentication in the login process, which aims to increase layered authentication in the login process so that unauthorized persons do not easily gain access to existing devices, networks, databases, or sensitive information. Active monitoring of website logs, where by monitoring and analyzing logs, such as database logs, web server logs, firewall logs, and intrusion prevention system (IPS)/intrusion detection system (IDS) logs, aims to increase awareness of access anomalies in the system. Change passwords periodically, which aims to provide password updates so that data security is maintained. Implementing standardization of the use of characters in passwords, which aims to provide standardization of passwords so that they have adequate security. The general standard recommendation that can be applied is to consist of a minimum of 12 (twelve) characters, consisting of at least 1 (one) uppercase letter, lowercase letter, numbers, and special characters. Hashing passwords before saving to the database, which aims to provide security to the database, so that if there is a risk of database theft, sensitive information on passwords is not easily known.

CONCLUSION

From the implementation of the Wireshark application in data security analysis on the LMS website, it can be concluded that the HTTP protocol is very dangerous if it is used to write confidential personal information, especially usernames and passwords. The risk is very clear, where the posting method that Wireshark captures, user input, can be encrypted in the clear without encryption. To overcome this condition, several improvements to the system are recommended, such as the use of the HTTPS protocol, implementation of Multi Factor Authentication, website log monitoring and password management. The recommended password management is changing passwords periodically, standardization policies for using characters in passwords and password hashing. It is hoped that when the

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume xx, Number xx, month Year
https://doi.org/10.47709/cnahpc.v4i1.1345

Submitted : Jan 20, 2022
Accepted : Jan 25, 2022
Published : Jan 25, 2022

recommendations are implemented it will improve security on the LMS website and reduce risks in data communications. As a suggestion for website development, it is expected to check using Wireshark to determine the security of data traffic so as to provide more security for the developed application.

REFERENCES

Abdillah, M., Yudhana, A., & Fadil, A. (2020). Sniffing Pada Jaringan WiFi Berbasis Protokol 802.1x Menggunakan Aplikasi Wireshark. *J-SAKTI (Jurnal Sains Komputer Dan Informatika)*, *4*(1), 1–8. https://doi.org/10.30645/j-sakti.v4i1.181

Alexander, A. D., Salkiawat, R., & Warta, J. (2021). Perancangan Intrusion Detection System Menggunakan Honeypot pada Universitas Bhayangkara Jakarta Raya. *Cyber Security Dan Forensik Digital*, *4*(1), 33–37. https://doi.org/10.14421/csecurity.2021.4.1.2379

Fitriani, Y. (2020). Analisa Pemanfaatan Learning Management System (LMS) sebagai Media Pembelajaran Online Selama Pandemi COVID-19. https://doi.org/10.52362/jisicom.v4i2.312

Huzaeni, F., Gunawan, I., Purnomo, D. C., Yanti, M., & Krisdayanti, N. (2021). Analisis Keamanan Data Pada Website Dengan Wireshark. *Jurnal Teknik Elektro Smart*, *1*(1), 13–17.

Ihsana, A. N., & Maslan, A. (2020). Analisis Keamanan Jaringan dari Serangan Paket Data Sniffing di PT Raden Syaid Kantor Pos Piayu Kota Batam. *Computer and Science Industrial Engineering Journal*, *3*(5), 11.

Iqbal, H., & Naaz, S. (2019). Wireshark as a Tool for Detection of Various LAN Attacks. *International Journal of Computer Sciences and Engineering*, *7*(5), 833–837. https://doi.org/10.26438/ijcse/v7i5.833837

Luthfansa, Z. M., & Rosiani, U. D. (2021). Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet. *Journal Information Engineering and Educational Technology*, *5*(1), 34–39.

Malek, M. S. A., & Amran, A. R. (2021). A Study of Packet Sniffing as an Imperative Security Solution in Cybersecurity. *Journal of Engineering Technology*, *9*(1), 96–101.

Manoppo, V. A., Lumenta, A. S. M., & Karouw, S. D. S. (2020). Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi. *Jurnal Teknik Elektro dan Komputer*, *9*(3), 181–188. https://doi.org/10.35793/jtek.9.3.2020.29567

Maulana, A. R., Walidainy, H., Irhamsyah, M., Fathurrahman, & Bintang, A. (2021). Analisis Quality of Service (QoS) Jaringan Internet Pada Website e-Learning Universitas Syiah Kuala Berbasis Wireshark. *Jurnal Komputer, Informasi Teknologi dan Elektro*, *6*(2), 27–30. https://doi.org/10.24815/kitektro.v6i2.22284

Nitra, R. O., & Ryansyah, M. (2019). Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen. *Jurnal Sistem dan Teknologi Informasi (JUSTIN)*, *7*(1), 52. https://doi.org/10.26418/justin.v7i1.29979

Prayitno, A. (2019). Analisis Kinerja Trafik Web Browser Dengan Wireshark Network Protocol Analyzer Pada Sistem Client/Server. *Musamus Journal Of Research Information and Communication Technology*, *2*(1), 12–18. https://doi.org/10.35724/mjrict.v2i1.2603

Putri, D. D. (2018). Pengembangan Learning Management System Menggunakan Framework Codeigniter dan Angularjs di PT. XYZ. *Jurnal Sistem Informasi*, *14*(1), 17–27. https://doi.org/10.21609/jsi.v14i1.540

Rakhmawati, N. I. S., Mardliyah, S., Fitri, R., Darni, D., & Laksono, K. (2021). Pengembangan Learning Management System (LMS) di Era Pandemi Covid-19 pada Pendidikan Anak Usia Dini. *Jurnal Obsesi : Jurnal Pendidikan Anak Usia Dini*, *6*(1), 107–118. https://doi.org/10.31004/obsesi.v6i1.991

Riswandi, Kasim, & Muh. Fajri Raharjo. (2020). Evaluasi Kinerja Web Server Apache menggunakan Protokol HTTP2. *Journal of Engineering, Technology, and Applied Science*, *2*(1), 19–31. https://doi.org/10.36079/lamintang.jetas-0201.92

Susianto, D., & Rachmawati, A. (2018). Implementasi dan Analisis Jaringan Menggunakan Wireshark, Cain and Abels, Network Minner (Studi Kasus: Amik Dian Cipta Cendikia). *Jurnal Cendekia*, *16*(2), 120–125.

Yana, D., & Adam. (2019). Efektivitas Penggunaan Platform LMS sebagai Media Pembelajaran Berbasis Blended Learning terhadap Hasil Belajar Mahasiswa. *JURNAL DIMENSI*, *8*(1), 1–12. https://doi.org/10.33373/dms.v8i1.1816

* Corresponding author