Kazenas German Vladimirovich
Student
Ural Federal University
Russia, Yekaterinburg
Research advisor: Kovaleva Alexandra Georgievna

WIRESHARK: MORE ADVANTAGES THAN DISADVANTAGES

Abstract: *Wireshark is a widely used network protocol and packet analyzer. It is widely used for network analysis by many organizations and institutions. Wireshark is an affordable alternative to many expensive packet analyzers. This article highlights the main advantages and disadvantages of the popular Wireshark packet analyzer.*

Keywords: *Wireshark, packet analysis, networks, information security.*

Казенас Герман Владимирович
Студент
Уральский федеральный университет
Россия, г. Екатеринбург
Научный руководитель: Ковалева Александра Георгиевна
Кандидат педагогических наук, доцент
доцент кафедры иностранных языков и перевода УрФУ

WIRESHARK: БОЛЬШЕ ПЛЮСОВ ЧЕМ МИНУСОВ

Аннотация: *Wireshark является широко используемым анализатором сетевых протоколов и пакетов. Он широко используется для проведения сетевого анализа многими организациями и учреждениями. Приложение Wireshark является доступной альтернативой многим дорогостоящим анализаторам пакетов. В данной статье выделяются основные преимущества и недостатки популярного анализатора пакетов Wireshark.*

Ключевые слова: *Wireshark, анализ пакетов, сети, информационная безопасность.*

The modern world is unthinkable without computers. A man has reached out to the whole world with information networks. An infinite amount of information circulates between computers. Many people have no idea how data is transmitted between devices and how networks work. Nevertheless, since information in today's world is of strategic importance, society needs network technology specialists to ensure the security of data transmission. The lives of people, companies, corporations, and governments can depend on them.

Another category of users is hackers who use their knowledge of network technology to steal and destroy information. Thus, the damage from cyberattacks in 2018 amounted to 1.5 trillion U.S. dollars. Information defenders who counteract hackers should be able to understand when an intrusion occurs, be able to block it and, based on analysis, prevent similar incidents in the future.

Since most attacks are carried out over the network, it is important to know what information can and cannot be delivered to and from the computer. The packet analyzer can help you with these tasks. There are several such programs, each with its advantages and disadvantages, but this study is focused on one of them.

Wireshark is a traffic analyzer program for computer networks. Many scientific publications are revealing various functionalities of this software product. Systematization and generalization of the possibilities of using this program to solve the problems related to information security is the rational of my research.

The purpose of the study is to systematize the possibilities of using Wireshark software to solve various problems related to information security.

The main problem in the field of information security is to ensure the protection of data of Internet users, both individual and collective (various institutions, government agencies, etc.). The information is transmitted not only in the form of coded signals and protocols, not only in writing by e-mail, but also by voice and video messages. There are many methods of penetration testing and vulnerability checking

of computer networks, web sites, and intrusion prevention to obtain confidential information. Intrusion testing is an essential tool for maintaining network security.

These methods include Meta rally, W3AF, nipper studio, BackTrack, Skip Fish, Wireshark [4]. Compared to these methods, Wireshark has some advantages. The main purpose of the Wireshark program is to detect the extent to which the system is vulnerable to security breaches. There are the following advantages of Wireshark:

1. *Ease of use and availability of documentation*. Firstly, the program is available for free download from the site. Secondly, the Internet has a large number of manuals that disclose the mechanisms of working with this software product, as well as publications on ways to optimize the program Wireshark.

2. *The program supports many protocols:* ARP [1], IP, ICMP, TCP, UDP, DCCP, HTTP, HTTP2, FTP, PPP, ATM, and others.

3. *The application is compatible with any specific operating system*, in particular with Linux, Windows, Mac OS, FreeBSD operating systems [1].

4. *The program allows you to capture packets from the network, record data online and analyze them offline*. This feature of the application allows you to prevent and respond quickly to possible intrusions.

As noted above, an important feature of this program is the possibility of its optimization. This is because many other libpcap-based analyzers, including Wireshark, have weaknesses, namely loss of packets at Gigabit Ethernet speeds. To solve this drawback, there is a possibility of increasing the kernel-level buffer memory capacity [2] and using a multi-threaded approach, which reduces the number of dropped packets, supports buffering regardless of libpcap, speeds up the application response time and, in general, increases the performance of interception. Optimization of Wireshark is a good alternative to expensive commercial alternatives, such as Viavi Observer Gigastor.

Besides, the Wireshark program allows you to identify security flaws in the system at the user authentication level. Easy capture of unprotected packets that are transmitted between network cameras [3] and servers, allows you to detect the possibility of using backdoor [4, 5].

The HTTP POST request contains user credentials. This package can be easily detected with Wireshark. When applying the Follow TCP Stream option, the entire contents of the selected package are displayed. As a result, it is easy to find your username - email and password in the form of plain text [4, 5].

However, Wireshark can be used not only to provide security but also to hack into a particular network, as network packet analysis provides partial access to personal and location information.

However, to use Wireshark, it is necessary to know not only the structure of the application but also the principles of processing incoming packets by different OS levels, as well as the limitations of the physical components of the PC [2].

Thus, Wireshark can be an analog of commercial solutions. A large number of filters for fast packet search and analysis, open-source code, which allows you to increase the functionality of the program and customize it for specific purposes, undoubtedly make this packet analyzer a good tool for the use in various areas of network technology: network training, network security audit, network configuration.

REFERENCES

1. Shaoqiang Wang, DongSheng Xu, ShiLiang Yan. - Analysis and Application of Wireshark in TCPIP Protocol Teaching. // International Conference on E-Health Networking, Digital Ecosystems, and Technologies. / Текст: электронный. – 2010. – [p. 269-272]

2. Abes Dabir, Ashraf Matrawy. - Bottleneck Analysis of Traffic Monitoring using Wireshark. // Innovations in Information Technologies. / Текст: электронный. – 18-20 Nov. 2007. – p. 158-162.

3. Resul Das, Gurkan Tuna. – Packet Tracing and Analysis of Network Cameras with Wireshark. // 5th International Symposium on Digital Forensic and Security. / Текст:электронный. – April, 2017.

4. Sandhya S, Sohini Purkayastha, Emil Joshua, Akash Deep. – Assessment of Website Security by Penetration Testing Using Wireshark. // 14 the International

Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery. / Текст: электронный. – 06 – 07 January, 2017.

5. Pimjai Navabud, Chin-Ling Chen. – Analyzing the web mail using Wireshark. // 14 the International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery. / Текст: электронный 28-30 July, 2018. – p.1237-1239.