Academicia Globe:
Inderscience Research

ISSN: 2776-1010 Volume 3, Issue 10, Oct., 2022

ANALYSIS OF EXISTING THREATS AND VULNERABILITIES IN COMPUTER NETWORKS

Usmanbayev Daniyorbek Shukhratovich,
Tatu named after Muhammad al-Khorezmi, Assistant

Annotation
This article will focus on possible threats and vulnerabilities in computer networks. When comparing the internal and external vulnerabilities of the network, the shortcomings, vulnerabilities and threats contained in the protocols are caused precisely by which perimeter attacks are made. At the end of the article, suggestions and recommendations were made against these vulnerabilities.

Keywords: Tarmoq, protokollar, tahdid, zaiflik, tarmoq xavfsizligi, himoya

Disadvantages of Internal Network Protection

After the testing process carried out by an internal attacker in the systems under study, it was achieved to increase the privileges of critical critical systems and obtain maximum privileges in critical systems. This resulted in complete control of the corporate infrastructure in 71% of cases.
The most common defenselessness of internal network resources remains the use of dictionary passwords. This defect was found in all projects without exception. At the same time, in 91% of cases, the use of weak passwords for privileged accounts was determined. The level of internal network security is still considered to be low.
In some cases, protective measures are used that are not yet sufficient to combat the attack.

Package Filtering Problems

Package filters also have problems. Of course, the developers of firewalls may object to those who say that the number of connections is available on personal computers, but it will lie in the whirlpool.
It also requires a very good load when you set up a local network on a computer that looks at the Internet.
It takes a lot of memory and processor resources to filter out normal transport. In this case, the data is divided into multi-level packet hierarchy, and not by continuous flow through the network. Again, it can be written as follows: Ethernet / IP / TCP / UDP. One TCP / UDP packet is divided into many IP packets on the network, that is, in a state of confusion. The order of delivery of IP packages may not coincide with the order of "cutting" them in the TCP-package, and some IP-packages may disappear, and then the sender will send again and again.
TCP-connection installation is a multi-stage operation. This means that a package that works at the IP level can be a filter simplicity.
It is impossible to "close" the port at the IP level. In a somewhat simplified scheme, this can be expressed as follows: the sender crosses a library that divides the recipient into small parts, is arbitrarily mixed with each other, and the recipient collects this puzzle in its original form.

ISSN: 2776-1010 Volume 3, Issue 10, Oct., 2022

Among them is censorship, which looks carefully for" political correction "and destroys it, or sends it" on the top floor". Obviously, if censorship (the same firewall) does not fully collect TCP packages, it will not notice anything suspicious. Theoretically, you can put the firewall at the level of TCP / UDP and filter already assembled packages, but then the hacker will be able to transfer the "raw" IP package, and the firewall will be in the folder.

At the Ethernet level, maximum protection is provided when filtering packages. No hacker can bypass it if the firewall is built without errors.

Worst of all, the firewall cannot completely collect all the TCP segment and return the IP packages "up" until it checks it as "negative". Package filters, in turn, force the collection of incoming data and the wrong TCP to be filled with "quotes" or transfer the accumulated threads to zero.

However, this can be a very strong point from the operating system. The processor simply does not have time to process such a state, and inevitable brakes appear. In addition, all TCP / IP operating system settings will be useless.

In ordinary operating systems (LINUX, FreeBSD), the package filter is initially installed on the TCP/IP drive, and such problems do not arise. Some firewalls do not filter packages according to the criteria of ports or IP addresses, but analyze them to verify compliance with QRM standards or to exploit the worm content or various vulnerabilities of client applications. For an uncomplicated user, this is attractive, but in fact all this is complete nonsense. Most attacks are usually carried out through TCP / IP packets.

Let's move on to shortcomings and weaknesses. Obviously, no firewall has the ability to know how to sign vulnerabilities that are not yet known, and therefore need to be updated from time to time.

If it is updated, then such a firewall does not require, and if it is not, then nothing can help. In short, it becomes a short circle.

In addition, it is impossible to check the contents of packages at the IP level. Most scans also require time and OS resources (especially if filled with polymorphic packets), and we are usually silent about heuristic analyzers. Checking the contents of the packages in the Modem connection is not yet clear, but there will be a tunnel function in the channels.

This is not an excuse to reject firewalls. They are absolutely necessary, but they should not rely on those tasks that they cannot solve. After all, no one wants to turn a submarine into a helicopter. And even if such a assembly is still created, its technical characteristics will not remain high. As a result, the submarine layer requires high density and strength (otherwise, an order to descend to a depth), and the helicopter must carry out its weight as light as possible. Firewalls here. protected by protected ports.

The package-filter hides special nodes of the local network from the "outside world". Antiviruses occupy aggressive applications.

Academicia Globe:
Inderscience Research

ISSN: 2776-1010 Volume 3, Issue 10, Oct., 2022

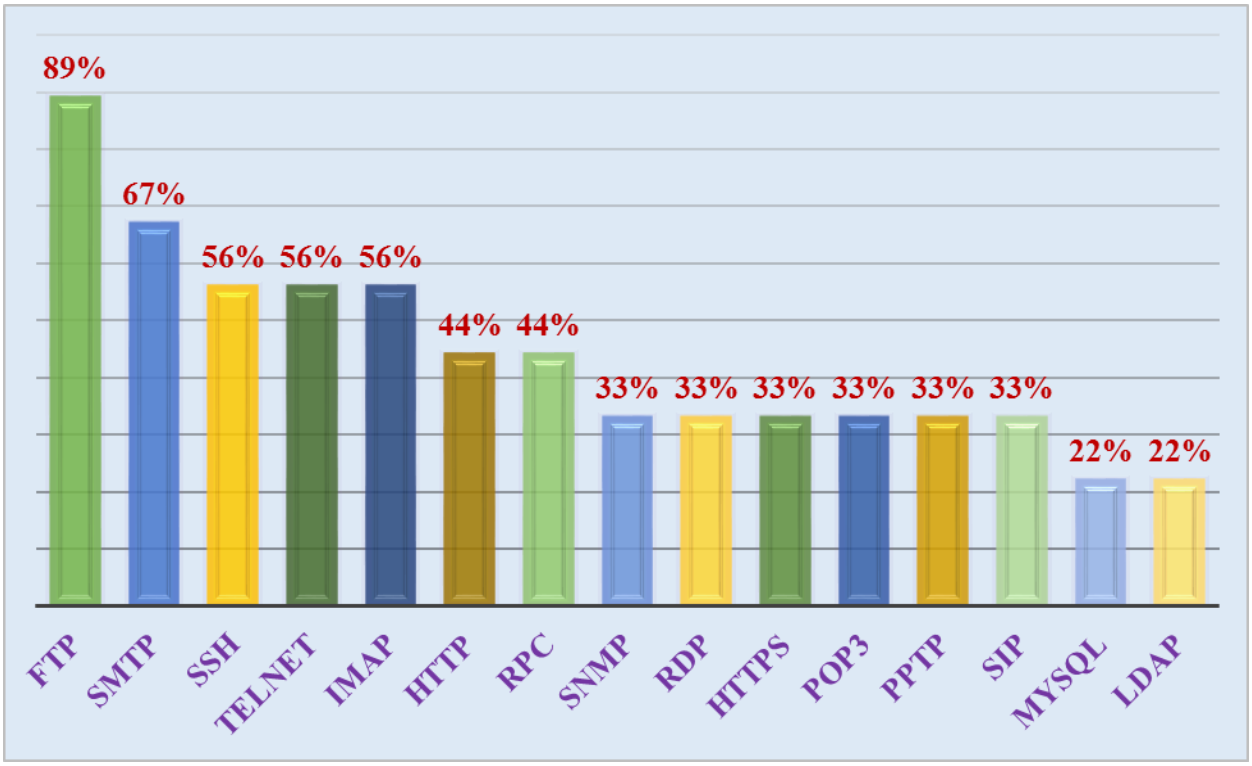
The most common vulnerabilities in the network perimeter since 2021:

- Weak versions of software in perimetric nodes, errors that intruders use to attack;
- Use of open data transfer protocols (Telnet, FTP, HTTP, etc.);
- The presence of external networks and network equipment with a limited amount of access by managers, as well as remote access interfaces that manage their servers.

The problem of using open data transfer protocols is still relevant. These shortcomings were identified in 89% of the systems and rose to the second line of the rating. It turned out that the FTP protocol was used in all such systems. Widely used protocols for accessing control interfaces are Telnet and HTTP protocols.

With the help of non-protection of data transmitted through these protocols, the sensitive attacker can suspend data, including the credentials of the privileged user, providing unauthorized access to resources.

The figure below presents the vulnerability coefficient of attack statistics in systems relative to protocols due to the vulnerability of protocols in the network perimeter.



1-rasm. Vulnerability indicators of network perimeter protocols

As noted, the high level of systems with interfaces for equipment management through the SSH (56%) and Telnet (56%) protocols for internet use has been preserved.

In a total of 44% of systems connecting from external networks to equipment management interfaces, the HTTP protocol was used.

On the perimeter of the network, the share of organizations available for connecting an external

ISSN: 2776-1010 Volume 3, Issue 10, Oct., 2022

network user to the SNMP service has significantly decreased (from 80% to 33%).

Disadvantages of Protecting Service Protocols

Each system being monitored included various deficiencies in the protection of service protocols such as ARP, STP, NBNS, LLMNR. Each project that conducted LAN network traffic analysis did not have any protection mechanisms against cache damage in ARP.In 73% of the analyzes, it was confirmed that the systems NBNS protocol does not have protection, and in 36% of the systems - the LLMNR protocol has vulnerability. Both protocols are used on Windows-based systems in situations where DNS servers are not available.In general, in recent years, the share of systems with weak service protocols has increased, it has become noticeable that the company's internal networks are not sufficiently protected from attacks against Channel and network protocols. If the use of these protocols is not necessary, they must be disabled, it is necessary to take precautions if necessary.

USED LITERATURE

1. Markelov O., Duc V. N., Bogachev M. Statistical modeling of the Internet traffic dynamics: To which extent do we need long-term correlations? //Physica A: Statistical Mechanics and its Applications. – 2017.
2. Платонов В. В., Семенов П. О. Обнаружение сетевых атак в компьютерных сетях с помощью методов интеллектуального анализа данных // Интеллектуальные технологии на транспорте. – 2016
3. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения. Труды СПИИРАН. 2016.
4. Pawar S.N. Intrusion Detection in Computer Network using Genetic Algorithm Approach: A Survey // International Journal of Advances in Engineering & Technology. 2013. vol. 6. Issue 2. pp. 730–736.
5. Barnes B. C., Sellers M. S. Getting Started with C++ //Introduction to Scientific and Technical Computing. – 2016. – С. 119.