Cyber security based on computer networks traffic – theoretical background

Adrian Florin Badea* **Victor Croitoru**** **Daniel Gheorghică***

Rezumat. Articolul descrie o prezentare generală a vulnerabilităților și posibilităților curente de exploatare ale rețelelor de calculatoare, posibilități de monitorizare a traficului de rețea prin interceptare și duplicare și modalități de analizare a traficului monitorizat.
Cuvinte cheie: securitate, securitate cibernetică, vulnerabilități, exploatări, monitorizarea traficului, analizarea traficului de rețea

Abstract. The paper presents an overview of the current computer networks vulnerabilities and exploits, possibilities of monitoring the network traffic, by intercepting and duplicating it and ways of analyzing the monitored traffic.
Keywords: security, cyber security, vulnerabilities, exploits, monitoring traffic, analyze network traffic

1. Introduction

Lately there was a very important development of computer network security systems. With the extraordinary expansion of the internet and of all the devices that connect to computer networks, the cyber security became critical for protecting the information and data hold and used in virtual environments.

Computer networks security is, at this moment, integral part of computer networks and it involves protocols, technologies, systems, instruments and techniques for securing and blocking the malicious attacks. Cyber-attacks increased considerably in the last few years.

Monitoring computers, systems and services that make up computer networks is achieved by collecting traffic from systems. Examination of the collected traffic allows a network administrator to maintain a robust network.

Regular collection of network information allows the creation of log files, records and reports of systems performance, so that the network can be monitored. With these data obtained, performance and infrastructure of the network can be optimized.

Vulnerabilities in computer networks are weaknesses which allows attackers to bypass the system's or network’s security. This grants the attacker access to critical information on victim’s computer. To exploit a vulnerability, an attacker must have at least one applicable tool or technique that allows connection to a system weakness. Vulnerability connection is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities.

* Kapsch S.R.L, Piaţa Montreal, nr. 10, World Trade Center, intrarea E, etaj 2, Sector 1, Bucureşti, mail: adrian.badea@kapsch.net

** Universitatea Politehnica Bucureşti, Facultatea de Electronică, Telecomunicaţii şi Tehnologia Informaţiei, Bd. Iuliu Maniu, nr. 1-3, Sector 6, Bucureşti, mail: croitoru@adcomm.pub.ro

2. Computer network security

2.1 Network security

Cyber security is, at this moment, an integral part of computer networks and involves protocols, technologies, systems, tools and techniques, to secure and stop malicious attacks. Cyber attacks have increased considerably in recent years.

Since the systems for collecting network traffic can be maliciously used to spy users or to obtain personal and confidential information such as passwords, it is important to maintain the possibility of securing the computer networks.
A good design is considered if security is implemented consistently, in the entire network, in as many ways and places as possible.

Controlled access - i.e. the idea of "Policy of Least Privilege"- the policy of fewer privileges is based on blocking anything and allowing only what is truly necessary.

To design a secure computer network is important to follow these principles [1]:

- specific security role – according to which the decision about the access and privileges is based on the role of the network users;

- user awareness – is essential for the network members to understand the importance of security. The vast majority of security problems do not occur because of malicious people, but due to misunderstanding the purpose of the security measures;

- monitoring - using systems to collect network traffic, which ensure the preservation of security and network protection from any attack;

- patching/upgrading – is a fundamental action in order to protect against possible vulnerabilities.

The most strategies for internal protection are based on policy implementation. Even a small computer network has a number of accounts and user groups with different levels of rights and permissions. Every time when a user has the right to access resources, it is possible to create potential network security breaches. To protect the network insider attacks, the network administrator must implement the appropriate measures to control passwords, user accounts, permissions and policies.

The passwords are the major key to protect the computer network. An user account with a valid password can penetrate any system. Even though, the user has limited permissions, security breaches can still be created. The users must choose strong passwords with at least 6-8 characters, including letters, numbers and special characters. Also, users must change their passwords at regular periods of time. Because most of the time users are using very simple passwords which can be hacked very easily or they simply forget to change the passwords, there are two alternatives to passwords: smart devices and biometric devices.

The access to user accounts must be granted only to the allocated persons, and these accounts must have the permissions to access only the resources they need and nothing more. The strict control of user accounts is critical to prevent unauthorized access. One of the best methods to control the accounts is the group. Rights and permissions are granted to groups instead of individual user accounts.

While the rights/permissions control the way in which users have access to shared resources, there are also a number of other functions that must be under control. Using policies, all network operating systems have different ways to control hundreds of security parameters (for example, permissions for users to install software or the specific users that may connect to different systems etc.). For security reasons, computer networks should be using different levels of protection, as represented in figure 1.

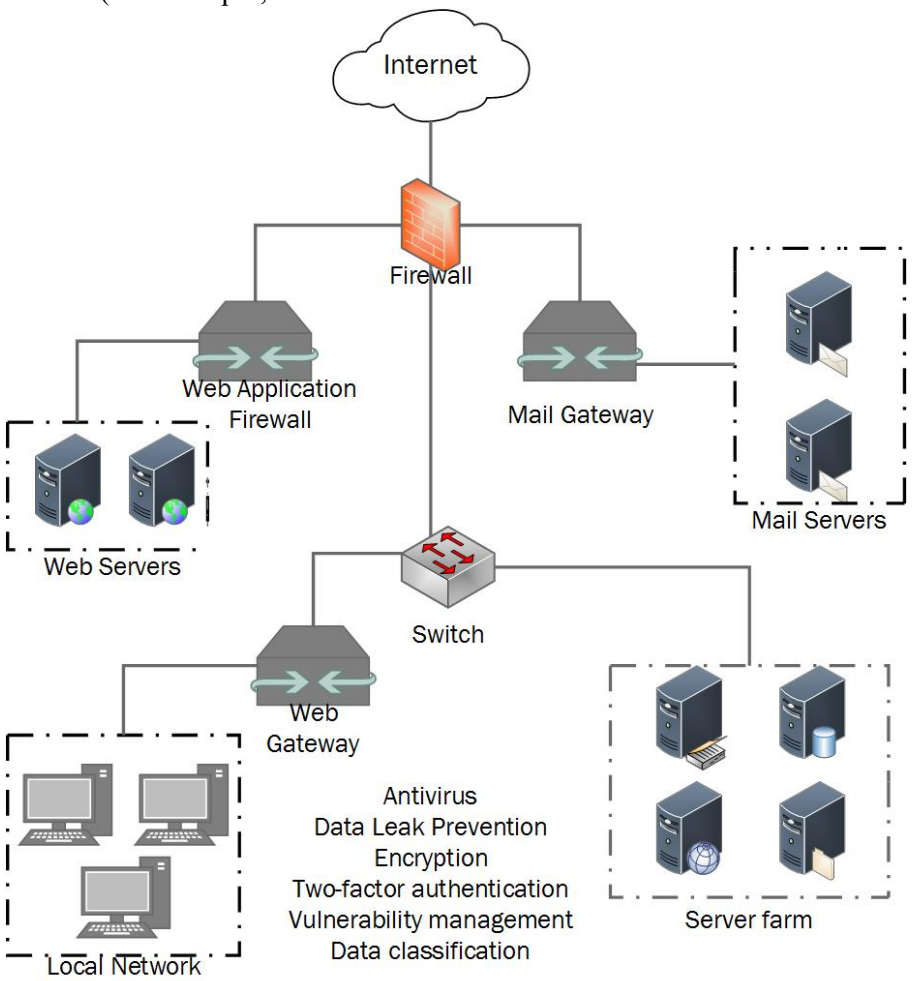


Fig. 1. Network using different levels of cyber security

2.2 Computer networks vulnerabilities

Computer users and network administrators can protect computer systems from vulnerabilities by keeping software security patches up to date. These patches can remedy flaws or security holes that were found in the initial release. Computer and network personnel should also stay informed about current vulnerabilities in the software they use and seek out ways to protect against them.

A typical day [2] at a company:
At every 1 minute a computer accesses a page with malicious content.
At every 3 minutes a bot communicates data to command and control center.

At every 9 minutes a highly risk application is accessed.
At every 10 minutes a known virus is downloaded.
At every 27 minutes an unknown virus is downloaded.
At every 49 minutes confidential data is sent outside the company.
At every 24 hours a computer is infested with a bot.

The main current cyber security risks and attacks [1] for which protection on networks is needed are:

Blocking a system service (Denial of Service - DoS) – represents an attack which tries to put the target in a blocking state so that the customers cannot use it anymore. There are a lot of ways that can set a blocking state to a target, like overwhelming the target with continuous connecting attempts.

Distributed blocking of a system service (Distributed denial of Service - DDoS) – is an attack which uses a collection of accomplices for attacking a target from multiple locations at once, without their notice.

SYN flood attack (Synchronization) - this takes place when a network is overwhelmed with SYN packets which initiates incomplete connection requests, so 8

UDP flood attack - similar with ICMP flood attack, UDP flood takes place when UDP packets are sent in order to slow down the system, so it cannot handle valid connections.

Port scan attack – takes place when packets are sent with different port numbers, in order to scan the available services, hoping that port will respond.

Ping of death - TCP/IP specifications require a certain packet size for transmitting data. Many implementations of ping command allows the user to specify a bigger size for the transmitted packet.

IP spoofing – takes place when an attacker tries to bypass the security of a network firewall, by using the IP address of a real user, e-mail address or the ID of a user. This is important when an attacker decides to exploit trust relationships between several computers.

Land attack – it is a combination of a SYN flood attack and IP spoofing attack and it takes place when an attacker sends fake SYN packets that contain the victim's IP address as both destination and source. The receiving system responds transmitting the SYN-ACK packet to itself and as a result it creates an empty session which lasts until the waiting period is reached. Bombing a system with empty sessions can overwhelm the system and it can block the target's system.

Tear Drop attack – exploits the reassembly of fragmented IP packets. In the header of IP, one of the options is the length value. When the sum between the length and the size of a fragmented packet differs from the next fragmented packet, the packets overlap and the server's attempts to reassembly the packets might block the system.

Ping Scanning - similar to port scanning attack, an attack with ping scan takes place when an attacker sends ICMP echo requests (or ping commands) to different IP addresses, hoping that it will receive a response back, and consequently, it will discover the IP address of a possible target.

Java/ActiveX/ZIP/EXE attack – Java or ActiveX malicious components can be hidden in web pages. When they are downloaded, these mini-applications can install a Trojan horse in the computer. Similarly, Trojan horses can be hidden in compressed files like .zip, .gzip and .tar and in executable files (.exe). By validating this function, it can block all the Java and ActiveX mini-applications contained by web pages and by .zip, .gzip, .tar and .exe e-mail attachments.

WinNuke attack – WinNuke is a hacker application whose only intention is to block any computer from the network that is running Windows operating system. WinNuke transmits data out of the band, usually on port 139 NetBIOS, to a host with an established connection, by introducing an overlap of a NetBIOS fragment which causes the computer to stop. This is the reason why NetBIOS should not be permitted in or outside the network.

Smurf attack – uses the ping command to target devices using an intermediate system, hiding the real attacking source.

Brute force attack – an attacker attempts to guess passwords using techniques like repeated attempts to open a work session on an account or using a dictionary with possible passwords.

Source routing – represents an option in the header IP which defines the way of directing the packets. When this option is activated on several firewall systems, rules are not used, granting an attacker access to the network. For example, the information held by the IP header, might contain different data to direct to another source IP address, than the original header.

ICMP flood attack – when ping commands overload a system with so many echo requests, so that the system uses all its resources to respond, until it cannot process valid network traffic.

Sniffing packets – using a device to intercept network traffic represents a passive attack which allows a network interface to be configured in promiscuous mode.

3. Traffic monitoring and pattern detection

3.1 Monitoring the information in computer networks

A sniffer is a device or a program that can collect network traffic, in order to decode it and to process it. The program will collect data which is addressed to other machines, saving it for future analyses.

The networks are using IP packets to send all their information. The transfer unit of a TCP/IP data packet is called IP packet. The IP packet is made of a header (which contains IP information) and the actual data (the only part of the IP packet relevant for higher levels).

In the easiest network example, when all the computers are sharing the same Ethernet cable, all the packets which are traveling between computers are detected by every single computer within the network. A hub transmits every packet to every node or machine from the network, and then each computer's filter remove all the packages that are not addressed to itself. The sniffer deactivates this filter to collect and to analyze some or even all the packets that are travelling the Ethernet cable; this depends on how the sniffer is configured. If the user

of computer A sends an e-mail to the user of computer B, the software installed on computer C can passively intercept the communication packets, without the knowledge of the two users. This sniffer is very hard to detect because it cannot generate network traffic on its own.

A safer environment is represented by a switched Ethernet network. Unlike a central hub, that transmits all the network traffic to all machines, a switch acts like a distribution device: it receives packets directly from the computer that generates them and it sends them only to the computer which is addressed.

There are many possibilities of avoiding the protocol used by a switch. A procedure, called ARP poisoning, can make the switch believe that the message is addressed to the sniffer and not to the computer with the real destination. After collecting the data, sniffer can forward the packets to the real destination. Another technique (MAC flooding) seeks to send lots of physical MAC addresses to the switch, in a short period of time, so that the switch change to fail-open mode. In this way, the switch starts to act as a hub, by transmitting all the packets to all the machines to assure that traffic reaches the destination. Both techniques – ARP poisoning and MAC flooding – generate traffic signatures which can be detected with the right software.

These programs might be used also on internet to capture data transmitted between different computers. The packets send to internet must travel very long distances, passing hundreds of routers. The sniffer can be installed at any point along the transmission path or on a server, which acts like a gateway that collects personal information.

Sniffing programs existed for a long period of time in two forms: commercial sniffer, used to monitor and troubleshoot the network and underground sniffer, used by hackers.

A sniffer is not only an instrument used by hackers. It can be used to troubleshoot the networks and also for many useful purposes. On the wrong hands, this software can capture personal and confidential data.

The flexibility of sniffers assumes:

- analyzing problems of a network;

- detecting the attempts to access the network;

- gathering and reporting the network statistics;

- obtain information in order to perform a network intrusion;

- filtering suspicious network traffic content;

- troubleshooting client/server communication.

Used maliciously, sniffer can spy the network users in order to collect personal and confidential information, like passwords.

Given that a sniffer can be used maliciously, the most efficient way to protect a network is by encryption. When an encryption algorithm is used, no packets can be read / decoded on other place than that indicated in the destination address. The sniffer can gather information, but their content is indecipherable. This thing shows how necessary it is to use only secure websites

when sending important information, like names, addresses, passwords or credit card data.

a. Sniffing in routed networks

• *Monitoring in promiscuous mode*

To use this monitoring possibility, the promiscuous operating mode must be available on the network adapter. In this mode, the network adapter arbitrarily accepts all the packets passing through the network segment. In a network that uses hub, it is enough for the network adapter to be configured in promiscuous mode in order to have access to all the traffic generated by the local network, because a hub is rather a primitive device. When a packet has been received on a specific port, the hub retransmits the packet on all the other ports.

• *Monitoring internet traffic in routed networks*

Most local networks are routed networks that are using devices like switches and routers. In such a network, when a packet arrives on a particular port, this is retransmitted on a different single port, to the computer which the original packet was intended. Switches maintain a MAC address and port table associated to each of these addresses. When a packet is received, switch validates the destination MAC address of the recipient from the table and selects the port on which the packet can be routed. The newest switches are using a port that can be configured so that all packets to pass through this specific port. This port is called "port mirroring", "Switched Port Analyzer (SPAN)" or "Roving Analysis Port".

• *Monitoring internet traffic in routed networks, using ARP-Spoofing technique*

This technique is using the ARP protocol weaknesses. ARP protocol is used in LAN to gather MAC addresses for their corresponding IP addresses. When a computer from the local network exchanges data with another computer from the internet, the local computer needs the router's MAC address, and the router in turn needs the MAC address of the local computer. In order to obtain the MAC address, the router sends a broadcast message, in the whole network, which contains the IP address for which the MAC address is needed. Being a broadcast message, all the computers from that network will receive the message. When such a message is received, the computer's operating system compares the IP address contained in the message with its own IP address and if they match, the computer sends its own MAC address to the router. To minimize the number of ARP interrogations, the operating systems are using cache memory.

ARP-Spoofing technique is based on the fact that the ARP protocol does not use any type of protection for possible frauds of the MAC addresses, so that anyone can use the router's MAC address as its own MAC address. Only the MAC address owner should respond to broadcast messages, but there is no method to prevent another computer from the network to stop answering to such interrogations.

b. Sniffing in wireless networks

A sniffer for wireless networks is a packet analyzer. It can be software or hardware specifically designed to intercept data

transmitted over the wireless network and to decode data; it is made in a readable format. Sniffers for wireless networks are able to analyze the particular packets of the wireless networks. These can monitor, intercept and decode data for: troubleshooting network problems, for monitoring activity and the security of the network, for vulnerability assessment, for traffic filtering and for identifying various encountered problems.

Wireless sniffers can also be used to initiate attacks over network. These can be used also to steal data and passwords of user accounts.

There are two possibilities for sniffing in wireless networks: monitoring mode and promiscuous mode. In monitoring mode, a wireless sniffer is capable to collect and to read data without transmitting data by itself. In promiscuous mode, a wireless sniffer is capable of reading all the data that pass through an access point.

3.2 Analyzing traffic in computer networks

Analyzing traffic [3] represents the process of listening and investigating network traffic. Analyzing the network provides an understanding of network communications in order to identify performance problems, to locate security breaches and to observe the behavior of applications.

The tools used to analyze traffic are usually sniffer devices. These devices can be hardware or software.

Many of the problems possible to occur in a network can be caused by the TCP/IP protocol or by specific applications.

Before analyzing traffic to identify problems, the administrator needs to know what is considered normal in a communication of the network.

When a client communicates with a specific server, the TCP/IP protocol uses a process of resolution based on several steps highlighted by figure 2.

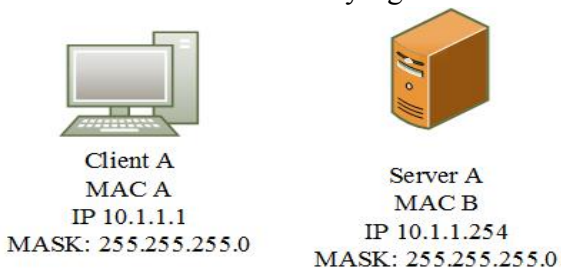


Fig. 2. The necessary data communication between client and server

This process includes the following steps (see figure 3):

- define the source and destination ports used by the application;

- identifying name with an IP address;

- if the target is on the local network, obtain the hardware address (MAC address);

- if the target is not on the local network, identify the nearest router to obtain the access path to the target;

- if the target is not on the local network, identify MAC address of the router.

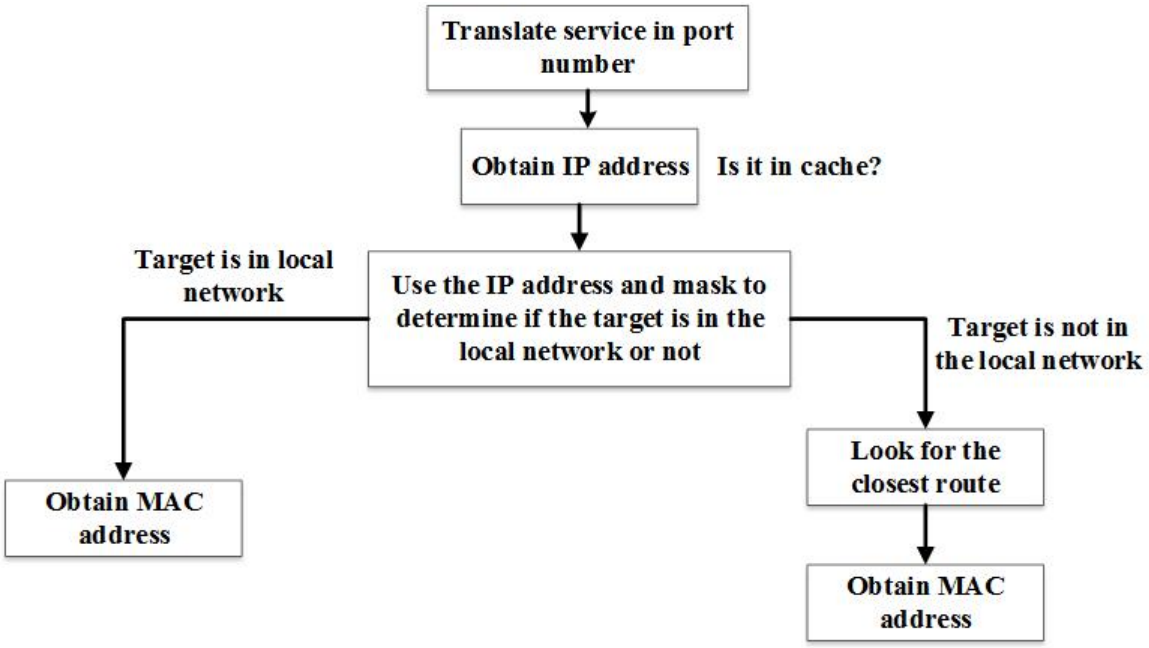


Fig. 3. The communication resolution process between client and server

When it is desired to identify the route of the target which is in the local network, the user first compares its own network address with the network address of the target, such as to determine whether the target is on the same network or not.

If the destination is a local device, the client should obtain the MAC address of the target. First it checks the cache memory, to see if the ARP information already exists. If not, the client sends a broadcast ARP message to search the MAC address of the target. After receiving an ARP response, the client updates its ARP cache. This may cause extra traffic on the network.

If the target device is in another network, the client must identify the route by setting the nearest router. The client searches the local routing tables to determine whether the input is a computer or a network for target. If none is available, the client looks for a default gateway. This process cannot cause extra traffic on the network.

In the last stage, the client must identify the MAC address of the nearest router or of the default gateway. The client first checks the ARP cache. If the information is not in cache, the client sends a broadcast ARP message to find the MAC address of the router and then updates its cache. This process may cause extra traffic on the network.

Wireshark [4] is the most used system for collecting and analyzing network traffic. Available free of charge, Wireshark can be used on many platforms. It has become a standard for analyzing computer network traffic. With the expansion of internet and networks based on TCP/IP model, Wireshark was used increasingly more for collecting, troubleshooting, and helping network administrators to understand the problems they may face.

For port spanning the principle used is to locate the device that needs to be monitored, to connect another device to a switch and to

configure the port for the device being monitored.

Usually, “port spanning” technique is used to configure the switch to submit a copy of the traffic obtained from all the configured ports to the monitored port. On the monitoring port, a program like Wireshark is used to collect, process and analyze data (as shown in figure 4). This method can be used only if the switch is hardware equipped with a span port.

By this, an administrator can easily monitor: LAN ports, WAN ports, server ports, routers, or any other ports of devices that are connected in the network.

There can be used tap or span ports to listen to a VLAN traffic. The destination port must coincide with the interface on the switch that is monitored by Wireshark. In order to see the VLAN tags, Wireshark interface does not need to be configured on the switch as a member on the same VLAN.

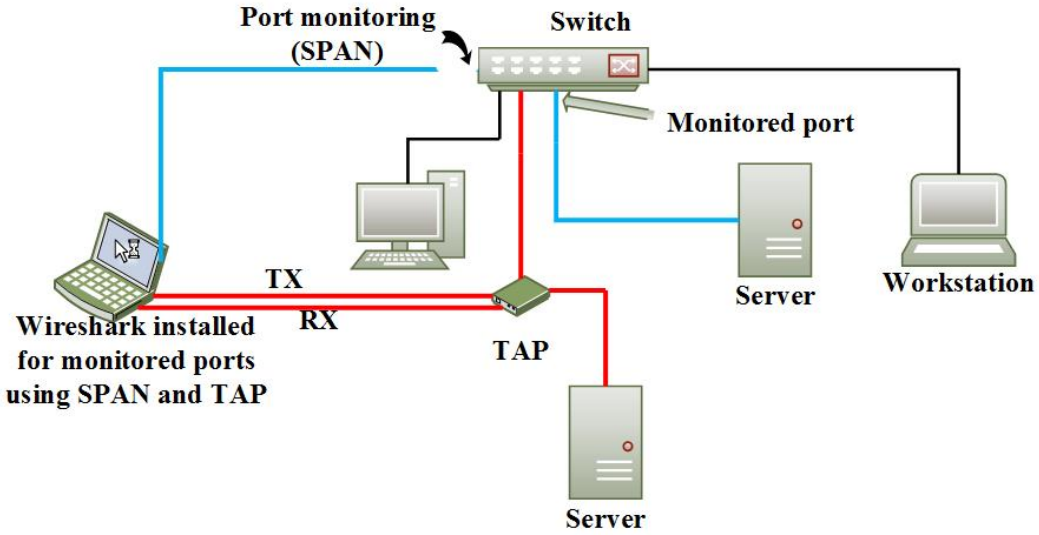


Fig. 4. Monitoring traffic in routed networks using TAP devices and SPAN port

Filters that can collect data are based on tcpdump syntax. This syntax appears in the libpcap/WinPcap library.

Tcpdump is used for capturing data packets transferred over the network in the following cases: to design networks/protocols, to check if some network services are properly running, to troubleshoot, to monitor and to make statistics based on traffic. The captured packets can be displayed selectively in text mode, on the console terminal or saved to a file. In addition, the output of tcpdump application can be viewed using Wireshark application.

Tcpdump acquires network packets captured through the second OSI layer interface, corresponding to a local network interface. By default, package collection involves intercepting all the packages, whether or not they are intended for the host on which the application is currently running.

For data collection, Wireshark uses Berkeley Packet Filters. Filters are capturing packets quite easily using host source and destination. The engine that captures events compares conditions with the actual MAC address and it only considers the relevant ones. For filtering hosts, when a hostname is

introduced, Wireshark will translate the name into an IP address and will capture packets that refer to that address.
Layer 4 protocols, TCP and UDP are protocols that interconnect applications. Node on a certain part (web client for example) sends messages to the other side (web server for example) to request permission to connect to the server. Processes codes that send the request and also the processes that receive the request are called port numbers. Both the TCP and the UDP port numbers indicate the application code that is used. Using packet capture, packets can be filtered from/to specific applications and also with certain specific flags. An example of a traffic capture using Wireshark program is shown in figure 5.

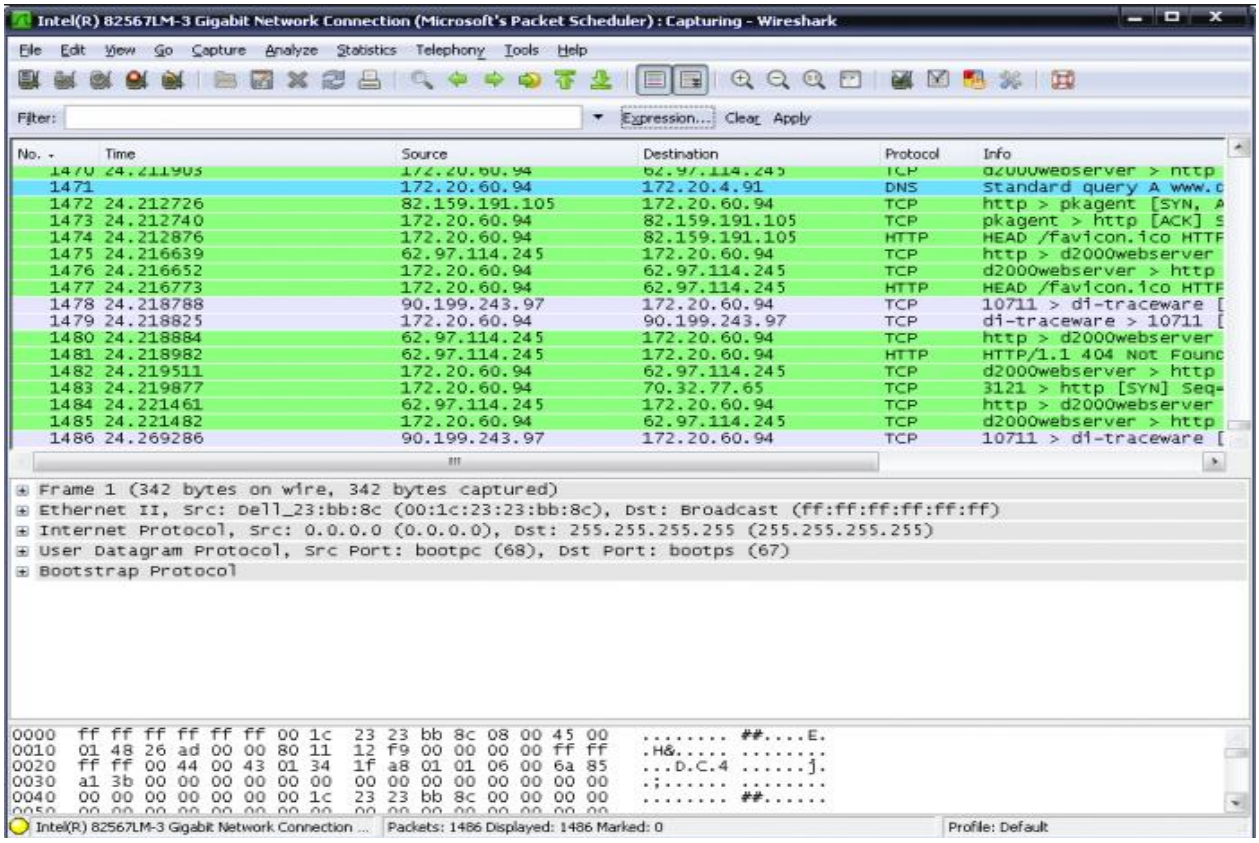


Fig. 5. Traffic capture using Wireshark program

NetFlow is a Cisco proprietary network protocol used for data collection and monitoring network traffic generated by routers and switches which support this technology.
NetFlow can analyze a large volume of traffic to determine from where the traffic came into the internal network, where it goes and the overall generated traffic. Before this innovation, in order to monitor network performances, Simple Network Management Protocol was used, which although has the necessary facilities to plan the capacity, and cannot characterize network traffic used by applications. NetFlow allowed visibility at the packet level and even visibility at the byte level to understand which IP addresses are the

sources for traffic and which applications generated all the traffic. A traffic flow (represented in figures 6, 7 and 8) will have the following information about the traffic

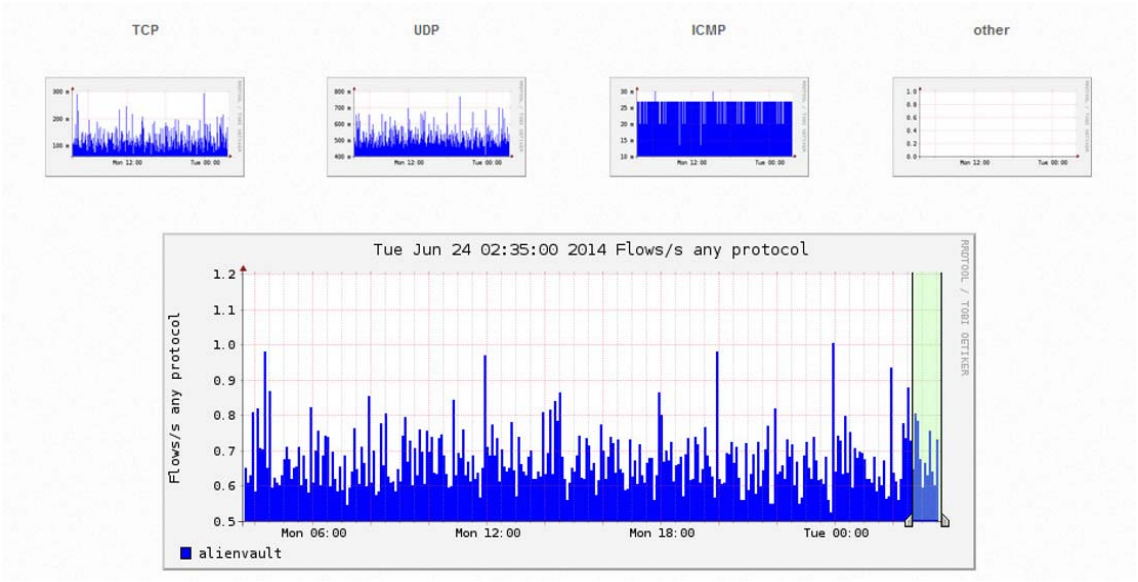
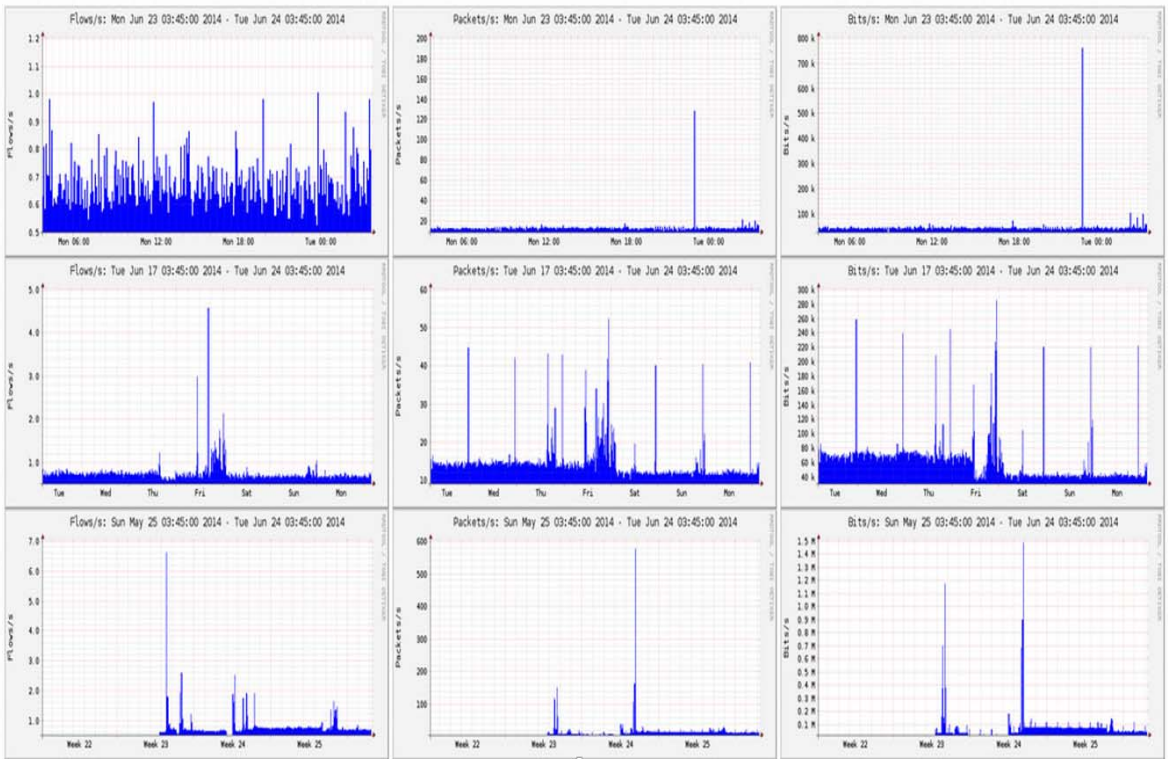


Fig. 6. Flows per second for all the protocols collected (including TCP, UDP and ICMP) using NetFlow



a. b. c.

Fig. 7. Data flows (a), packets (b) and bits (c) per second measured in different weeks

session: network interface, source IP address, destination IP address, IP protocol, source port, destination port, TCP flags, the total number of packets in the flow, the total number of bytes in the flow, the number of packets per second, the number of bits per second, the average number of bits per packet, the duration (milliseconds).

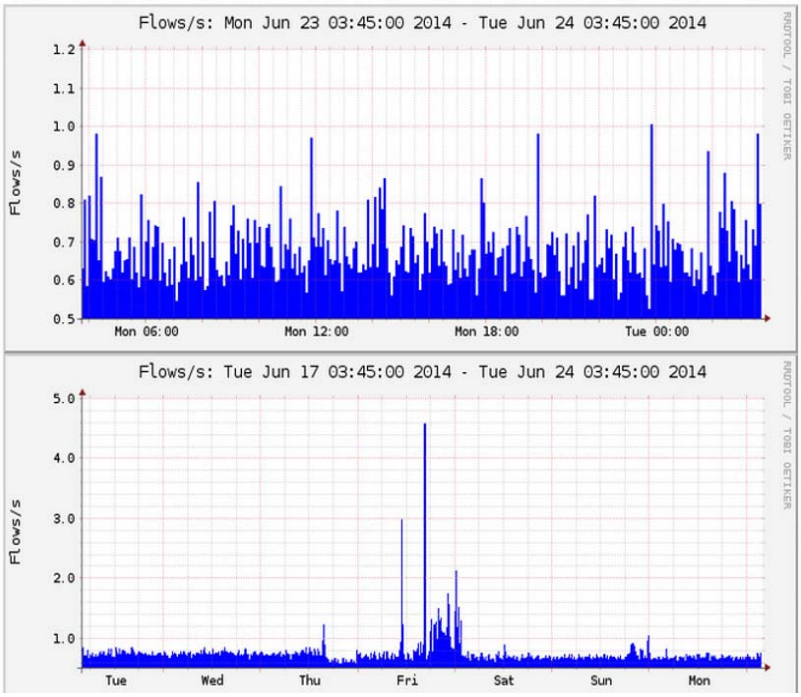


Fig. 8. Data flows per second in different days and hours

To take advantage of this protocol, the collecting system needs a switch that is configured to use the SPAN port. The collection of the network traffic using NetFlow is represented in figure 9.

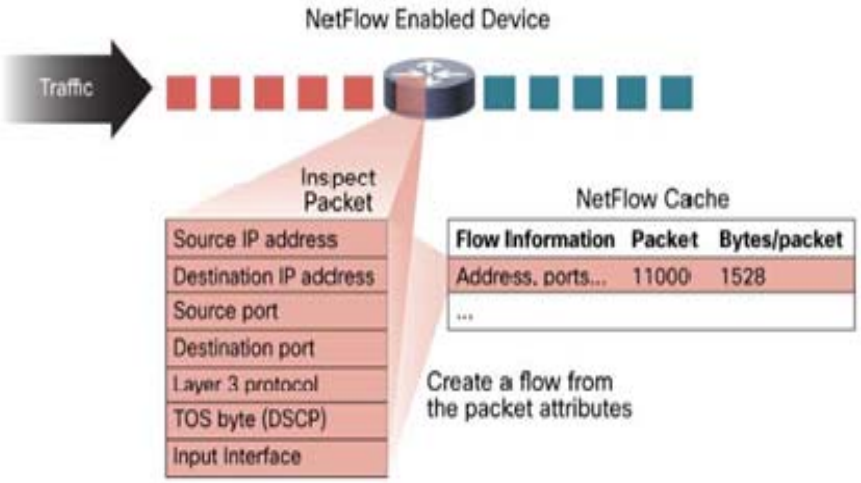


Fig. 9. Collecting network traffic using NetFlow [5]

4. Conclusions

Cyber security became critical for protecting the information and data used in virtual environments. Vulnerabilities allow attackers to bypass the system's or network's security. This grants the attacker access to critical information on victim's computer. This is why monitoring computers, systems and services that make up computer networks is a challenging and complex task. Monitoring is achieved by collecting traffic from systems using sniffers on both routed and wireless networks.

For a network administrator it is very important to be able to analyze the network traffic in order to identify performance problems, to locate security breaches, to assess the vulnerabilities and to observe the behavior of applications. The analysis can be made with both Wireshark software and using the NetFlow protocol. By analyzing network traffic, administrators should be aware of the behavior of the users in order to detect possible security issues.

References

[1] Thomas T., *Network Security first-step*, Cisco Press, Indianapolis, USA, 2004

[2] Product documentation, *Check Point Security Report 2014*, Check Point, San Carlos, USA, March 2014

[3] Dean T., *Network+ Guide to Networks*, Fifth edition, Course Technology, Boston, USA, 2010

[4] Chappell L., *Wireshark Network Analysis*, Second edition, Chappell University, San Jose, USA, 2012

[5] Product documentation, *Introduction to Cisco IOS NetFlow*, Cisco, San Jose, USA, May 2012