SocioBrains
ISSN 2367-5721, JOURNAL HOMEPAGE: WWW.SOCIOBRAINS.COM
INTERNATIONAL SCIENTIFIC REFEREED ONLINE JOURNAL WITH IMPACT FACTOR
ISSUE 56, APRIL 2019

IDENTIFICATION OF ACTIVE HOSTS IN THE COMPUTER NETWORKS AND EVALUATION THE NETWORK SECURITY AGAINST MODERN TYPES OF CYBER ATTACKS

Abstract: In this paper an identification of active hosts in the computer networks and evaluation network security against modern types of cyber attacks is made.

Author information:

Petar Boyanov
Associate Professor, PhD,
Lecturer in Department
"Communication and Computer Technologies"
at Konstantin Preslavsky University of Shumen
✉ peshoaikido@abv.bg
Bulgaria

Keywords:
Cyber attacks, Computer and network administrators, Computer resources, Host, LAN, Network security, Protocols, Security, Vulnerability, WAN.

1. Introduction

To be carried out defined cyber attack is necessary strictly and to sequentially switch all phases of the attack. Incorrect performance of a phase leaves evidence and trace to analysts and computer and network security analysts to track down and catch the malicious perpetrator to answer the court institutions for their malicious acts. The phases of the cyber attacks are intelligence, network scanning, access, access control and concealment of the tracks [1], [2], [3], [4], [5], [8], [11], [29], [30], [31], [32].

Scanning is one of the most important phases of detailed information gathering for the malicious perpetrator. In the scanning process, the attacker collects information about certain logical IP addresses that are accessible through the global Internet space, operating systems and system victim architecture, and on-site services running on each computer [6], [7], [9], [22].

The purpose of the scan is to detect vulnerable communication channels and examine listening ports to exploit them with malicious software tools over the computer network. During the scanning phase of the attack, the offender performs any scanning mode to gain unauthorized access to his victim. The attacker tries to find much more important information about his victim by understanding the type of operating system used, the services being run, and individual system configuration errors [21], [26], [27]. The attacker then forms a strategy for cyber attacks, based on the various facts learned during the scanning phase. The different types of scanning are [14], [15], [16], [17], [18], [19], [20], [23], [24], [25], [29], [30], [31], [32]:

- **Port scanning**: Port scanning is a process to check the victim-machine services by sending a message sequence to penetrate the selected computer system [28]. Port scanning involves connecting to the TCP and UDP ports of the victim machine to determine whether services are running or in a listening state. Occasionally, active services that work in a listening state may allow unauthorized user access to computer systems because they are incorrectly configured, or the running software has many vulnerabilities [11], [12], [13].

- **Network scanning**: Network scanning is a procedure for identifying active hosts in the computer network and assessing network security.

- **Vulnerability Scanning**: Vulnerability Scan is a method used to check the state of vulnerability of the computer system by identifying existing vulnerabilities. The vulnerability scanner consists of a

scan tool and a catalog. The catalog consists of a list of common files with all the known vulnerabilities and another sheet of all open exploits. Vulnerability scanners check for secretly installed files, operating system recovery, and directory relocation [10], [14], [17], [19], [29], [30], [31], [32].

When talking about computer systems and networks, ports and services can be represented as the doors and windows of a house through which the perpetrator wants to gain access. A basic rule for computer systems is that the more open ports are in the system, the greater the probability of operating the system. Sometimes, however, in some computer systems there are less open ports in contrast to other machines, but even with a few open ports there is a much greater risk of vulnerabilities. Because even with an open port, the attacker will be able to exploit open vulnerability, thus ensuring access to his victim [15], [16], [17], [22], [23], [24], [25], [27].

Scanning phase

Scanning is the phase just before the actual cyber attacks. At this stage, the attacker uses the collected intelligence information to identify specific vulnerabilities. Scanning can also be seen as a logical expansion of active intelligence, and in practice most cyber-doers do not distinguish between scans and active intelligence. The attacker collects critical information about the architecture of computer systems, routers, switches, firewalls, sensors to detect and prevent malicious network packets being sent through simple tools such as tracert for Windows-based operating systems. This network tool is extremely useful because it shows all the paths (jumpers) that pass the sent reconnaissance packet. In this case, each jump is a physical device called an IP address router through which the packet passes. Each router reduces the packet's lifetime by one unit to prevent packet storms and seizures in the computer network [1], [2], [4], [6], [8], [10], [14], [17], [29], [30], [31], [32].

Port scanners are used to detect listening ports, which in turn provide information about the type of services running on the victim's computer machine. The main security equipment against port scanners is the exclusion of system services that are not mandatory for execution. Another very important security technique is the application of packet filtration of all traffic in the computer network. However, most professional hackers and malicious users may use software tools to determine the rules applied to package filtration.

The most commonly used software tools are vulnerability scanners that have the ability to scan thousands of known vulnerabilities of the victim. This, in turn, gives an advantage to the attacker because he has to find a single system gap and exploit this vulnerability. Most organizations that use intruder detection systems should be very vigilant because hackers can use avoided techniques with modified software tools. The most serious attacks are the external denial of services that can either deplete resources or stop services launched on the victim's machine [3], [5], [9], [12], [18], [20], [21], [25], [26], [28]. Services can be stopped by the appropriate adjoining process by using a logical or time bomb, reconfiguring, and collapsing the software system. The resources can be exhausted locally by loading and filling the outgoing network connections with a lot of redundant information [29], [30], [31], [32].

Objects of network scanning

The most important objects in the scanning phase are [1], [2], [3], [11], [13], [15], [19], [22], [23], [24], [27]:

- Determination of running and running systems in the computer network [1].
- Detection of open ports [2], which will help the attacker determine the best way to drill the selected system.
- Disclosure of the installed operating system of the victim-machine, which is called "making a basic footprint of the victim". In this way, the perpetrator can formulate a strategy based on the existing vulnerabilities for this operating system.
- Detecting startup and listening services in the victim's machine. This gives the attacker an indication of the vulnerability of the service to exploit in order to gain access to the system.
- Detecting the victim's network IP address [3].
- Disclosure of certain software applications and versions of commonly used services [6].

- Detection of vulnerabilities in all running computer systems on the network. This can be extremely important for testing the hosts' security of future malicious scans and cyber attacks.

Network Scanning Methodology

In proven practice, any attacking hacker follows a particular sequence to scan a particular computer network. The steps for scanning the computer network are [1], [2], [3], [4], [5], [6], [11], [29], [30], [31], [32]:

- Check for active and running computer systems. Perpetrator can begin by checking for running systems in the computer network.
- Check for open ports. Once the operating systems are detected, the attacker will look for open ports to understand which services are running in the systems. This is a vital step because most of the services may have vulnerabilities.
- Taking a footprint for your operating system. The next phase includes identifying the type of installed operating system in the computer network.
- Scan for vulnerabilities. Vulnerability identification in the victim's operating system is the next step. The hacker can exploit these vulnerabilities during the attack.
- Testing the computer network. An attacker can choose to actively test the network or unnoticely track the traffic on the network. The anonymous Internet surfing technique makes the process of tracking user activity extremely difficult for the perpetrator.

Verification for operating computer systems using network search equipment

The search engine "PING" is a basic network scanning technique that determines the scope of IP addresses of the working hosts. The single "PING" indicates whether the scanned host exists in the computer network. The search engine, however, consists of many ICMP (Internet Control Message Protocol) echo queries sent to multiple hosts on the computer network. If the given IP address is active, then the victim host will return the ICMP echo response [13], [16], [19].

The term "PING" is a process where the attacker's computer system sends a single packet over the network to a specific network IP address. This packet consists of 64 bytes, of which 56 bytes are used for data, and the other 8 bytes are used for header header information. If the network connections are stable and good and the victim's machine is working, then a response packet is sent to the attacker. The term "PING" also gives information about the jumps numbers that are between two or more hosts and the amount of time that the packet must traverse the network distance. This distance is also called a full journey time. Thanks to this technique, the attacker can also get the names of the hosts [1], [3] [5], [6], [9], [10], [14], [16].

It should be noted that disclosure of active hosts in the selected computer network is the main step in the process of unpredicted penetration of the resources of a given computer system or network [22].

Transmission Control Protocol (TCP) is a protocol-oriented protocol that establishes a connection before actually packet data between two applications. This network connection is possible through the three-way handshake process. This handshake is encrypted to establish a network connection between protocols.

The very process of establishing a connection consists of the following:

1. The host "Petar" source sends a synchronization pack SYN (Synchronize) to the recipient host "Nikolay" to establish a TCP connection.

2. Once the recipient host "Nikolay" has received a synchronization packet, the TCP session begins by sending a packet containing timing flags for synchronization and confirmation to its source.

3. Receiving the package containing the synchronization and confirmation flags means that the first synchronization packet was sent correctly.

4. To complete the established connection, the source host "Petar" sends a packet containing a confirmation flag to the network connection.

This allows the communication between the source and the recipient while either of them sends a finishing packet or packet to interrupt the established network connection.

The all computer networks in the Cisco Packet Tracer version 6.2.0.0052 programming environment are simulated.

On fig.1 the general scheme of the computer networks is shown. On fig.2 and fig.3 successfully established connection between two hosts is illustrated.

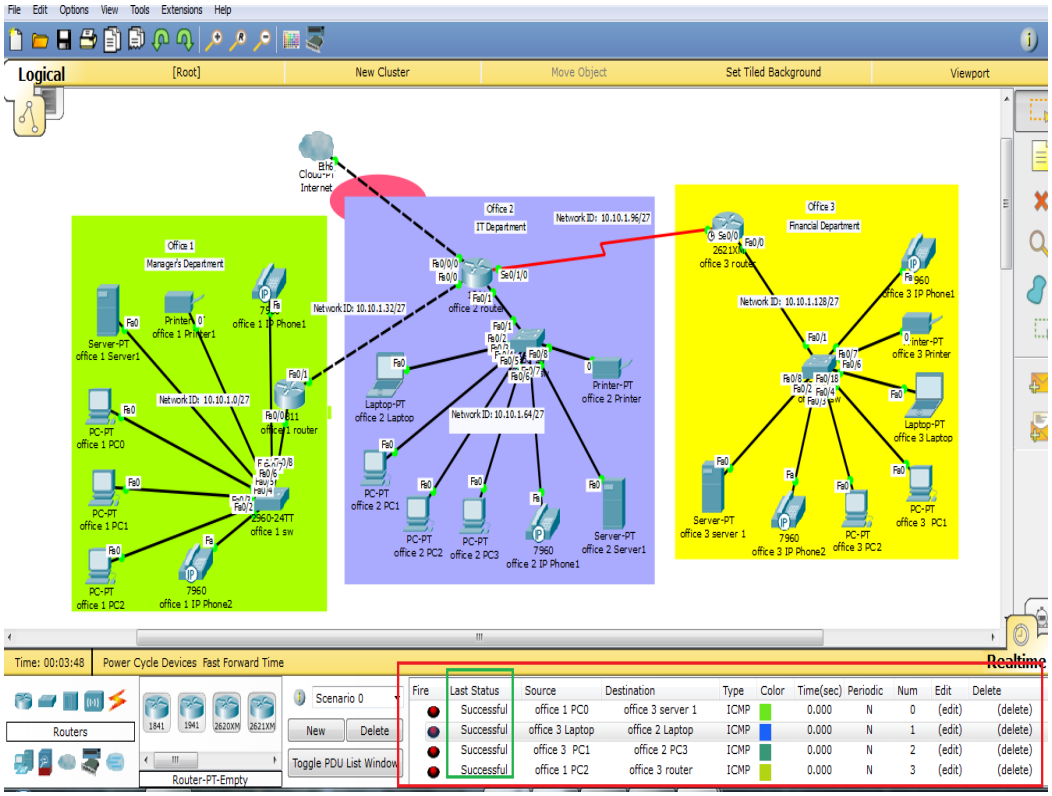

Fig.1. General scheme of the computer networks

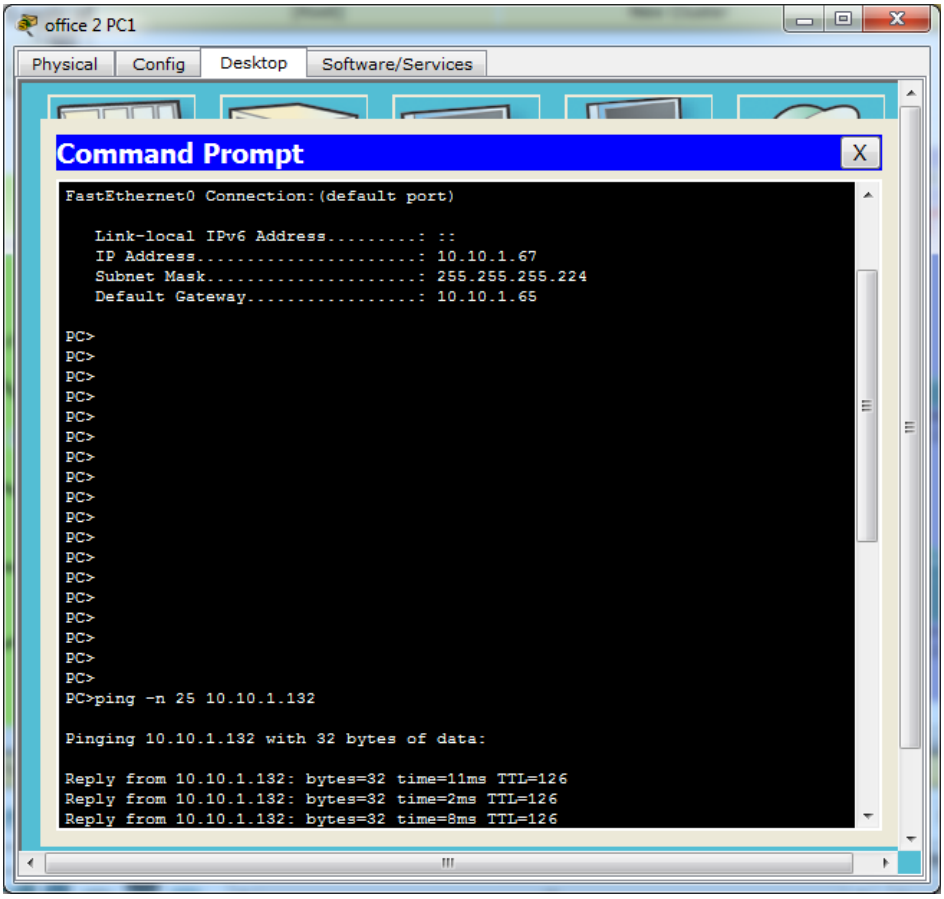

Fig.2. Successfully established connection between two hosts

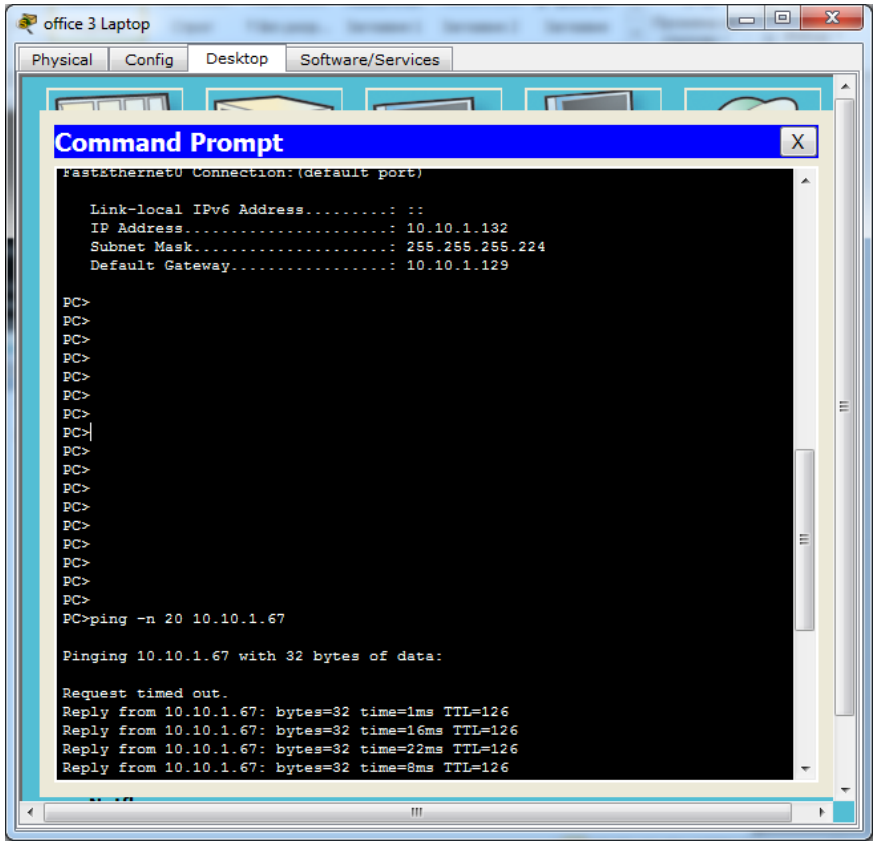

Fig.3. Successfully established connection between two hosts

ATTENTION: All the experiments and research in this paper are made in a specialized computer laboratory at the Faculty of Technical Sciences of the Konstantin Preslavsky University of Shumen, consisting of several hosts and a home-based local computer network consisting of four hosts. Everything illustrated and explained in this paper is for research purposes and the authors are not responsible in cases of abuse.

3. Conclusion

System administrators must constantly be aware of various new exploits and constantly monitor their computer networks. Installing new updates and fixes for an operating system is a necessary step to reduce the risk of exploiting vulnerabilities.

Unfortunately, security is not the most important priority for software developers, so various add-ons [3], [9] are available on the market after the release of a software product. Error checking in these software applications can be very low or almost absent, which in turn will lead to buffer overflow attacks.

Software developers often use free and free libraries and licensed code from other sources in their programs. This means that a large portion of many software chunks will have almost the same structure and algorithms, and if vulnerabilities [22] are found in that code, then all these pieces will be at risk.

The problem in the whole situation is that most software developers leave their system libraries and codes unchanged [7]. Programmers need to rewrite and edit all system libraries and codes at a certain time interval to reduce the vulnerability exploitation process.

Although a particular computer system appears secure and secure, it can only be exposed to an incorrect configuration. System administrators should very carefully configure their computer systems and always know what is being done on them. It is necessary to make a simple and effective configuration, eliminating all unnecessary services and software products and tools.

References:

1. Barry B. I., Chan H. A., Intrusion detection systems, Handbook of Information and Communication Security, Springer Berlin Heidelberg, ISBN: 978-3-642-04117-4, pp. 193 – 205.

2. Beale J., Foster J. C., Snort 2.0 Intrusion Detection, Syngress Publishing, 2003, ISBN: 1-931836-74-4, pp. 650.
3. Bejtlich R., The Practice of Network Security Monitoring: Understanding Incident Detection and Response, No Starch Press, 2013, ISBN-13: 978-1593275099, pp.376.
4. Berenjkoub, Mehdi S. H. F. H., A Taxonomy for Network Vulnerabilities, International Journal of Information & Communication Technology, May 2010, Vol.2, №1, pp. 29-44.
5. Fry C., Nystrom M., Security Monitoring, O'Reilly Media, 2009, ISBN: 978-0-596-51816-5, pp. 248.
6. Hekmat S, "Communication Networks", "PragSoft Corporation", USA, 2005 g.
7. Helmer, Guy, et al. "A software fault tree approach to requirements analysis of an intrusion detection system", Requirements Engineering 7.4 (2002): 207-220.
8. Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks. Informatsionnые tehnologii i bezopasnosty, Zhurnal Akad. nauk Ukrainы., Spets. vыpusk, Kiev, 2013, Str. 79-86.
9. Nachev A.I., G. Zhablyanova, Analitichen model na efektivnost na sistema za zashtita na informatsiyata, Voenni tehnologii i sistemi za osiguryavane na otbranata, Sofia, 2014.
10. Nachev A. I., St. Zhelezov, G. Zhablyanova, Sintez na sistemi za zashtita na informatsiyata pri zadadeno nivo na efektivnost, Voenni tehnologii i sistemi za osiguryavane na otbranata, sofia, 2014.
11. Ogletree, Terry William, ed. Upgrading and repairing networks. Que Publishing, 2004.
12. Stanev St., Szczypiorski Krzysztof., Steganography Training: a Case Study from University of Shumen in Bulgaria, Intl Journal Of Electronics And Telecommunications, 2016, Vol. 62, No. 3, Pp. 315-318, Manuscript received September 7, 2016; revised September, 2016, DOI: 10.1515/eletel-2016-0043.
13. Savov, I., Edin pogled varhu protivodeystvieto na hibridnite zaplahi v Evropeyskia sayuz, mezhdunarodna konferentsia „Asimetrichni zaplahi, hibridni voyni i vliyanieto im varhu natsionalnata sigurnost", Nov Balgarski universitet, mart 2018 g., ISBN 978-619-7383-09-6, s. 179-185.
14. Savov, I., Edin pogled varhu sashtnostta na kiberprestapleniyata, spisanie „Politika i sigurnost", VUSI, 2017, ISSN 2535-0358, s. 36-47.
15. Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.
16. Neykova, M., Vavezhdaneto na vtoro nivo na mestno samoupravlenie – osnovna antikrizisna myarka, godishnik BSU, tom XXVII str. 161.
17. Neykova, M., Protsesat na detsentralizatsia na Republika Bulgaria, godishnik na BSU, str.161.
18. Neykova, M., Prilaganeto na printsipa na subsidiranostta – osnoven instrument za regionalizatsia i detsentralizatsia , Yuridicheski sbornik na TsYuN pri BSU, str. 161.
19. Sotirov, Ch., Preventsia na uchilishtnoto nasilie chrez elektronni sredstva, Nauchni trudove tom 50, seria 6,2 RU - 2011. ISSN 1311-3321.
20. Sotirov, Ch., Relationship between the social development and motor activity of the child. SocioBrains - international scientific online journal publisher: www.sociobrains.com., Issue 24, August 2016, ISSN 2367-5721.
21. Sotirov, Ch., Stoyanova, I., Savremenni tehnologii v preduchilishtnoto obrazovanie. Godishnik na ShU „Ep. K. Preslavski", tom XX D,2016 ISSN 1314-6769.
22. Hristov, H., Scanning for vulnerabilities in the security mechanisms of the hosts in the academic institutions and government agencies, Mathematical and Software Engineering, ISSN 2367-7449, Vol. 4, No. 1, 2018, pp. 1-6 (available at: http://varepsilon.com/), indexed in Russian Science Citation Index, (RINTs: Nauchnaya эlektronnaya biblioteka eLIBRARY.RU), VINITI RAN Эlektronnыy katalog nauchno-tehnicheskoy literaturы VINITI.RU, National Centre for Information and Documentation (Bulgaria), Google Scholar, OpenAIRE, Polish Scholarly Bibliography (PBN), Index Copernicus International, ROAD, the Directory of Open Access scholarly Resources, DOAJ, Directory of Open Access Journals.
23. Kantardzhiev, I., Stanev, S., Hristov, H.,Otnosno finansovoto osiguryavane na deynostta na firmeno kontrarazuznavatelno zveno. Sbornik nauchni trudove - Nauchna konferentsia s mezhdunarodno uchastie "MATTEH 2018" - 25-27 oktomvri 2018, ISSN: 1314-3921, t.2, ch.1, 2018, s.96-108.
24. Hristov, L., Stanev, S., Hristov, H., Sredstva za zashtita na chuvstvitelnata informatsia na firmata ot vatreshni zlozhelateli (insayderi). Sbornik nauchni trudove - Nauchna konferentsia s

mezhdunarodno uchastie "MATTEH 2018" - 25-27 oktomvri 2018, ISSN: 1314-3921, t.2, ch.1, 2018, s.109-115.
25. Trifonov T. , Bateriite na prenosimite kompyutri - problemi i reshenia, Sbornik nauchni trudove MATTEH 2018, tom 2, chast 2, str. 37-45, Universitetsko izdatelstvo ShU, 2018, ISSN: 1314-3921.
26. S. Kazakov, T. Trifonov, I. Tzonev, Probabilistic-temporal characteristics in a three level centralized computer structure, Proceedings of the 10-th Baltic-Bulgarian Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics, June 2-7, 2014, Liepaya, Latvia, Riga.
27. Zh. Zhivkov, T. Trifonov, Meditsinskie mikrokommunikatsionnыe sistemы maloy moshtnosti, ispolyzuyushtie slozhnыe signalы, Proceedings of the 10-th Baltic-Bulgarian Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics, June 2-7, 2014, Liepaya, Latvia.
28. Trifonov T., Analiz na proizvoditelnostta na prenosim kompyutar, oborudvan s poluprovodnikovo ustroystvo za sahranenie na danni, Godishnik na ShU „Ep. K. Preslavski", Tehnicheski nauki, Universitetsko izdatelstvo, Shumen, 2014 str. 27-42, ISSN 1311-834X.
29. Dimitrova, N., 2014: The motivation for effective study of technical and technological information assimilation. International Scientific Online Journal – ISSN 2367-5721 Issue 4, December 2014, www.sociobrains.com, pp 94-99.
30. Dimitrova, N., 2015: Operationalize the aims of technological education International Scientific Online Journal. Issue 16, December 2015, www.sociobrains.com pp. 48 –53.
31. Dimitrova, N., 2014: Role of informatization in technological education and information culture of students International Scientific Online Journal, Issue 2, October 2014, www.sociobrains.com pp. 26-30.
32. Dimitrova, N. Prinosat na tehnologichnoto obuchenie za sahranyavane na balgarskite natsionalni traditsii. – Godishnik na Shumenskia universitet „Episkop Konstantin Preslavski", T. HH D, Nauchni trudove ot konferentsia „Inovatsii v obrazovanieto", 30 septemvri – 02 oktomvri 2016, Pedagogicheski fakultet, Shumen, Episkop Konstantin Preslavski, 2016, 686 – 690.