Journal scientific and applied research, vol. 14, 2018
Association Scientific and Applied Research
International Journal

Original Contribution ISSN 1314-6289

EDUCATIONAL EXPLOITING THE INFORMATION RESOURCES AND INVADING THE SECURITY MECHANISMS OF THE OPERATING SYSTEM WINDOWS 7 WITH THE EXPLOIT ETERNALBLUE AND BACKDOOR DOUBLEPULSAR

Petar Boyanov

DEPARTMENT OF MANAGEMENT OF SECURITY SYSTEMS, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712,115, UNIVERSITETSKA STR,

E-MAIL: peshoaikido@abv.bg

ABSTRACT: *In this paper an educational exploitation of information resources and invading the security mechanisms of the operating system Microsoft Windows 7 with the exploit EternalBlue and backdoor DoublePulsar is conducted.*

KEY WORDS: *Education, Exploit, Information resources, Security, Vulnerability, Windows 7, Windows XP.*

1. Introduction

Most of the cybercriminals are able to install different online applications into the computer and network systems of selected victims in determined government agencies, private organizations and academic institutions [6, 7, 8, 9, 10]. In addition to these applications some cybercriminals and malicious users send special IPv4 and IPv6 network addresses and web hyperlinks to the marked victims in order to gain an unauthorized access to the computer and network resources [6, 7, 8, 9, 10].

Unfortunately, most of the normal users have not the slightest notion that is the purpose of these sent IP addresses and fraud web hyperlinks and as result of this execution they shall become victims. Therefore, the whole set of confidential information could be stolen and public exposure to third parties. In this paper an exploitation of information resources and invading the security mechanisms of the operating systems Windows XP and Windows 7 with the exploit EternalBlue and backdoor DoublePulsar. The whole academic research and experiment in specialized computer laboratory in the Faculty of Technical

Sciences at Konstantin Preslavsky University of Shumen is conducted [6, 7, 8, 9, 10].

This paper is structured as follows. First, in section 2, a detail survey of the structure and functions for exploitation's process is made. After that, in section 3, the process of exploitation in the target hosts in the Wireless Local Area Network (192.168.1.0/24) is performed. The achieved results are presented in section 4. The final conclusions and recommendations are made in section 5.

2. Related work

In [1] a specific methodology for penetration tester and penetration testing team is given. Common hacking tools for Linux and Windows based operating systems by Fox, Erin, Jeremiah Bush, Sylvia Ashley, and Ian Webb are analyzed tested and evaluated [2]. In [3] the details and functions of the Metasploit Framework by Carlos Joshua Marquez are explained and tested. In [4] a brief description of the whole structure of the Metasploit Framework and Metasploit Project by H. D. Moore is presented and explained. In [5] several free and open source tools as well as techniques to simulate malicious cyber-attacks by Nishant Shrestha are illustrated and made.

3. Experiment

The experiment in a specialized university computer lab in the Faculty of Technical Sciences at Konstantin Preslavsky was made. All of the hosts in this lab were connected each other in Wireless Local Area Network (WLAN). The investigated computer network was consisted of 11 hosts and each of them was using a 150 Mbps High Gain Wireless USB Adapter TL-WN721N. In the computer lab a Cisco RV315W Wireless-N VPN Router has been used and configured. The Dynamic Host Configuration Protocol (DHCP) in the router's configuration has been configured on purpose each host in this computer lab to obtain a valid IPv4 addresses, network mask, DNS server addresses and default gateway. The network ID of this WLAN is 192.168.100.0/24. The research host was configured with the following IPv4 address 192.168.1.124/24 [6, 7, 8, 9, 10].

The name of the used the exploit was "EternalBlue". This exploit [2] in several security vulnerability databases was indexed. This exploit used vulnerability in the Server Message Block (SMB) protocol with version 1. This exploit caused critical damages to the selected computer and network system. The details of this vulnerability [5] were known as CVE-2017-0144. The backdoor DoublePulsar was used alongside with the exploit EternalBlue. Thanks to the DoublePulsar cybercriminals can obtain full unauthorized control and access of the information resources of the exploited operating systems - Microsoft Windows XP and Windows 7 [6, 7, 8, 9, 10].

The next step with the configuration of this exploit was connected. The following steps were made:

- SRVHOST was set on host with IP address 192.168.1.124 because this was the attacking host.
- SRVPORT was set on port 4444 because this exploit would be executed vie http protocol [4],[5].
- RHOST was set on host with IP address 192.168.1.134 because this was the victim host.
- PROCESS was set on the explorer.exe system file. This is shown of fig.1.

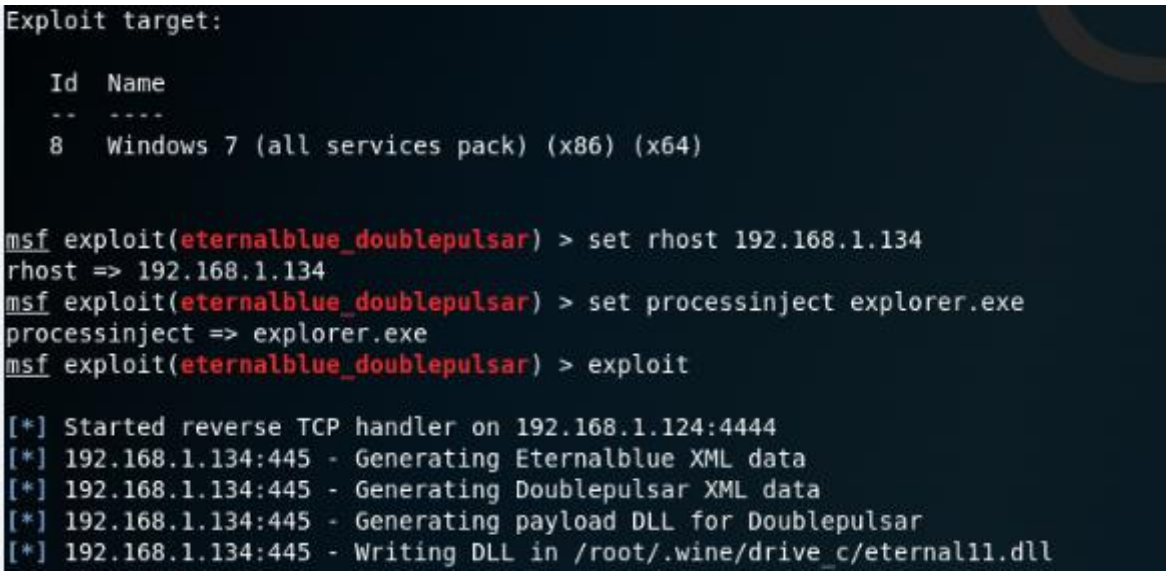

Fig. 1. Configuration of the exploit

4. Results

The attacking host (192.168.1.124) the operating system called “Kali Linux x64” has used. All studies in this article only with scientific research character were made. The author of the report is not responsible for cases of abuse [6, 7, 8, 9, 10]. Fig. 2 illustrates the successfully executed remote code on the host with IPv4 address 192.168.1.134.

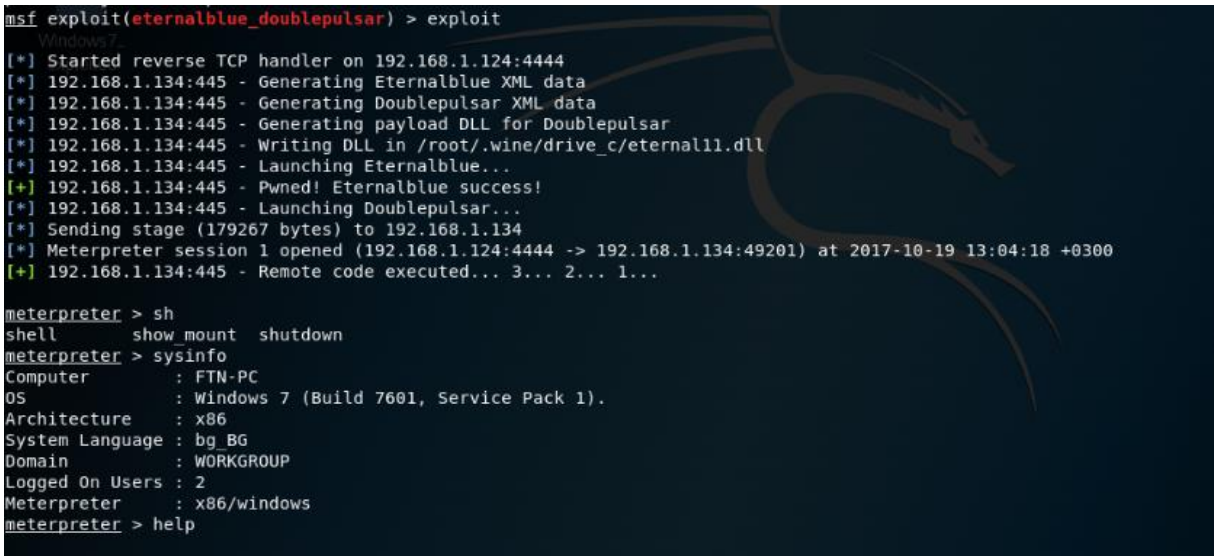

Fig. 2. Successfully executed remote code on the host with IPv4 address 192.168.1.134

From fig. 2 could be seen that the computer name was “FTN-PC”, operating system was “Windows 7 (Build 7601, Service Pack 1), architecture was “x86, system language was “bg_BG” and payload type (Meterpreter) is “x86/windows”.

Fig. 3 and 4 show all running processes in the exploited operating system with the command “ps”.

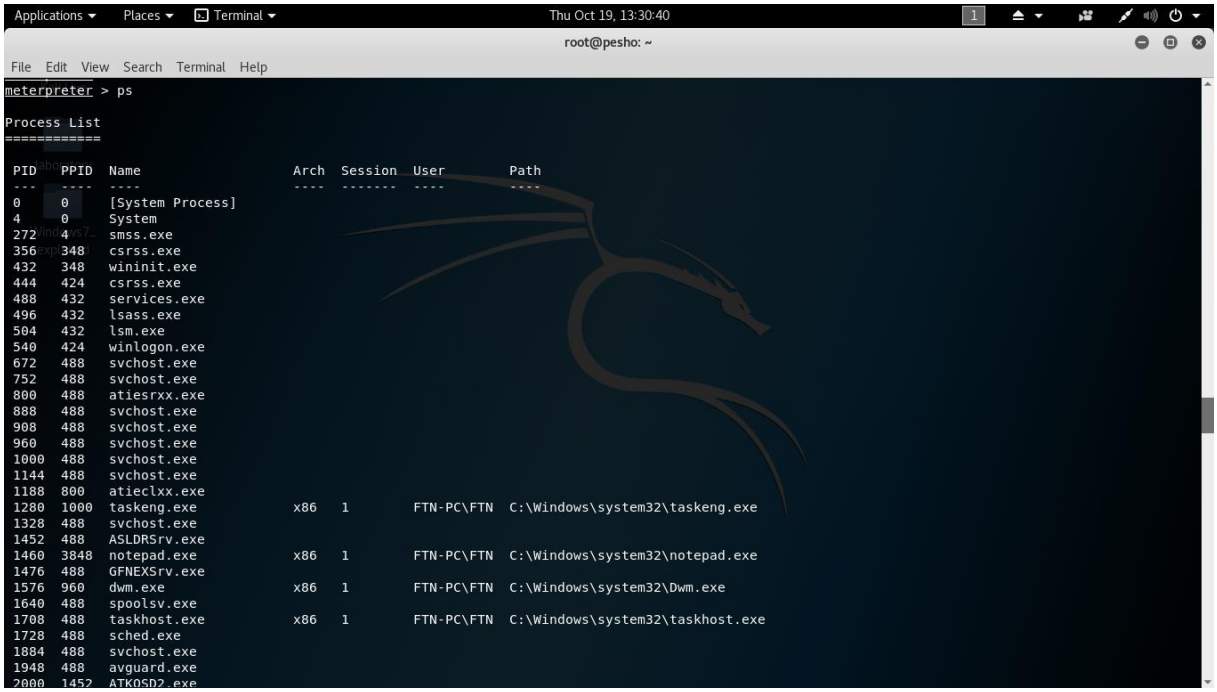

Fig. 3. All running processes in the exploited operating system

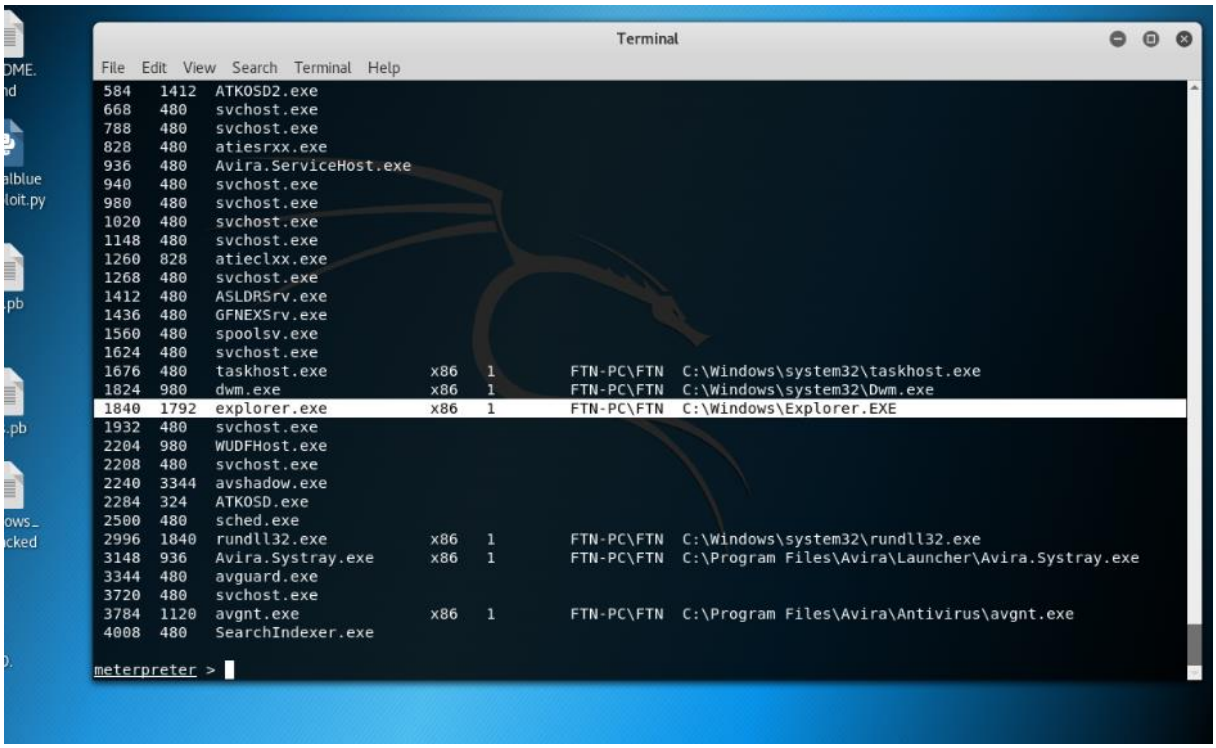

Fig. 4. All running processes in the exploited operating system (192.168.1.134)

The available targets of the exploit “EternalBlue” are the following:

- Windows XP (all services pack) (x86) (x64).
- Windows Server 2003 SP0 (x86).
- Windows Server 2003 SP1/SP2 (x86).
- Windows Server 2003 (x64).
- Windows Vista (x86).
- Windows Vista (x64).
- Windows Server 2008 (x86).
- Windows Server R2 (x86) (x64).
- Windows 7 (all services pack) (x86) (x64).

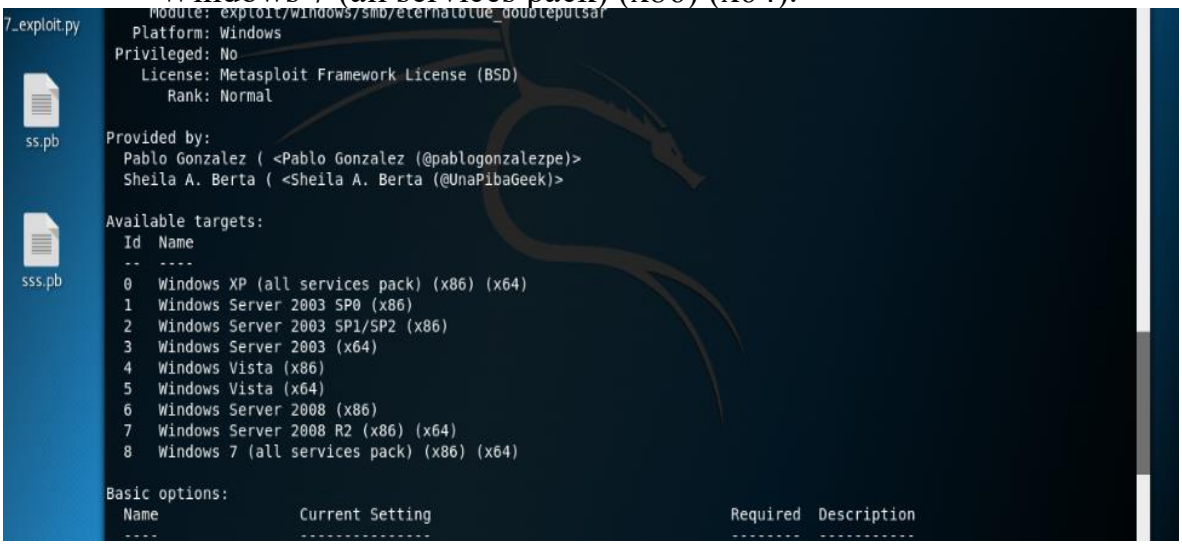

Fig. 5. All available targets of the exploit “EternalBlue”

The fig. 6 shows the successfully get current desktop of the exploited victim with IPv4 address (192.168.1.134).

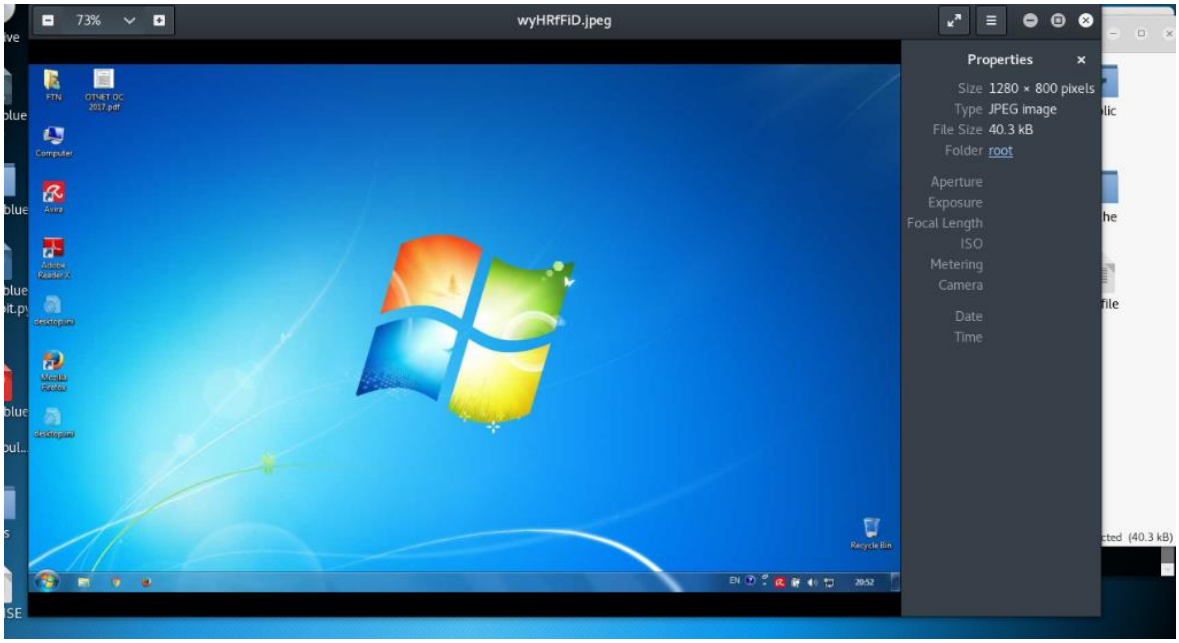

Fig. 6. Successfully get current desktop of the exploited victim with IPv4 address (192.168.1.134)

The fig. 7 illustrates the successfully executed command “dir” that lists all files and folders of the current desktop of the exploited victim with IPv4 address (192.168.1.134).

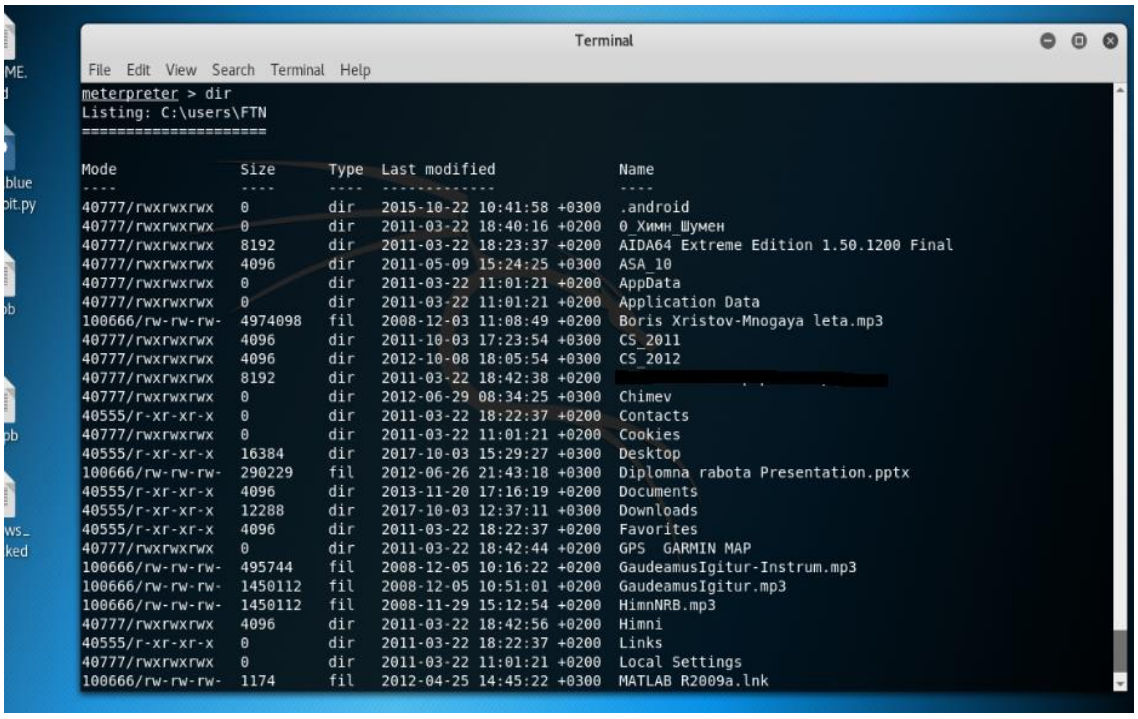

Fig. 7. Successfully executed command “dir” of the exploited victim with IPv4 address (192.168.1.134)

5. Conclusion

Thanks to the achieved results the security officers of automated information systems and security network administrators mandatory have to constantly install security updates on the operating system Microsoft Windows 7. The total security against this exploit is using the information of Microsoft Security Bulletin MS17-010. Thanks to this security bulletin the security network administrators can investigate and monitor the current appeared malicious exploits and backdoors in the cyberspace.

References:

[1]. Bhattacharyya, D., Alisherov, F. Penetration testing for hire. International Journal of Advanced Science and Technology, 2009, vol. 8, pp. 1-8.

[2]. Fox, E., Bush, J., Ashley, S., Webb, I. Common Hacking Tools for Linux and Windows, 2002, CS 581 Semester Project, pp. 1-17.

[3]. Marquez, J. An Analysis of the IDS Penetration Tool: Metasploit. The InfoSec Writers Text Library, 2010, pp. 1-6.

[4]. Moore, H. D. Metasploitation. In CanSecWest Security Conference, 2006, pp. 1-28.

[5]. Shrestha, N. Security Assessment via Penetration Testing: Network and System Administrator's Approach: Security, Network and System Administrator, Penetration Testing, Master's thesis, 2012, pp. 1-98.

[6]. Boyanov, P., Vulnerability penetration testing the computer and network resources of windows based operating systems, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), ISSN 1314-6289, vol. 5, 2014, pp. 85-92.

[7]. Boyanov, P., Zhaneta, T., An unauthorized penetration into computer system with activated firewall and antivirus software. Anniversary Scientific International Conference 45 Years Computer Sciences and Engineering Department 30 Years Computer Systems and Technologies Speciality, 27-28 September, 2013, ISSN 1312-3335, Varna, Bulgaria, Section 1 Computer systems and Networks, pp.41-46.

[8]. 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, (РИНЦ: Научная электронная библиотека eLIBRARY.RU), ВИНИТИ РАН Электронный каталог научно-технической литературы 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.

[9]. Hristov, H., The company security system – a contrivance to counteract to all possible encroachments, Journal Science Education Innovation, Konstantin Preslavsky University Press, ISSN 1314-9784, Vol. 3. 2014, pp. 104-111.

[10]. Hristov, Hr., A modern survey on problems of business organization's security, Journal Scientific and Applied Research, vol. 7, 2015, pp. 72-79.