Mathematical and Software Engineering, Vol. 4, No. 1 (2018), 1-6.
Varɛpsilon Ltd, varepsilon.com

Scanning for Vulnerabilities in the Security Mechanisms of the Hosts in the Academic Institutions and Government Agencies

Hristo Hristov

Department of Management of Security Systems, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, 9712 Shumen, Bulgaria, e-mail: hristov63@abv.bg

Abstract

In this paper a sophisticated investigation and scanning for vulnerabilities in the security mechanisms of the hosts in the academic institutions and government agencies is made. The port and network scanner are specialized software tools that can discover detail information about the selected target hosts such as open, filtered, closed ports and the whole computer network topology.

Keywords: Computer Network, Host, Ports, Scanning, Security, Vulnerability.

1. Introduction

Most of the cyber-criminals and malicious users discover vulnerabilities and holes in the started processes and services in the target operating systems of the victims. In most cases the victims are employees working in academic institutions and government agencies [6, 7, 13]. Because of ignorance or mistake for security officers of automated information systems and security networks administrators some network ports, processes and services are not being configured and as a result they operates in default open mode. Thanks to that the cyber-criminals uses specialized network scanning tools such as portscanners with what can discover and analyze each host in order to exploit the found vulnerability with the purpose of obtaining an unauthorized access to the computer resources of the victim [1, 2, 3, 4, 5, 8]

2. Experiment

The experiment in a specialized university computer lab 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 17 hosts and each of them was using a 300Mbps High Gain Wireless USB Adapter TL-WN822N. 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 192.168.1.0/24. The research host was configured with the following IPv4 address 192.168.1.124/24.

The attacking host an operating system called "Kali Linux x64" has used. The portscanner "Nmap" version 7.60 for operating software platforms x86_x64-pc-linux-gnu was used.

This network scanning tool consists of various scanning mode and in most cases can determine the network state of the victim. All studies in this article only with scientific research character were made. The author of the report is not responsible for cases of abuse.

3. Results

The first step is scanning the whole network ID - 192.168.1.0/24 for hosts in active network state. Figure 1 shows that 17 hosts are in active network state. Figure 2 illustrates the successfully executed command "nmap -T5 --packet-trace --reason --script default 192.168.1.0/24". This command aims to discover vulnerabilities with default loaded scripts. Figure 3 indicates that host with IPv4 address 192.168.1.91 has got 6 open ports and 994 filtered ports and this result was achieved thanks to the executed command "nmap -T5 --ip-options T 192.168.1.0/24".

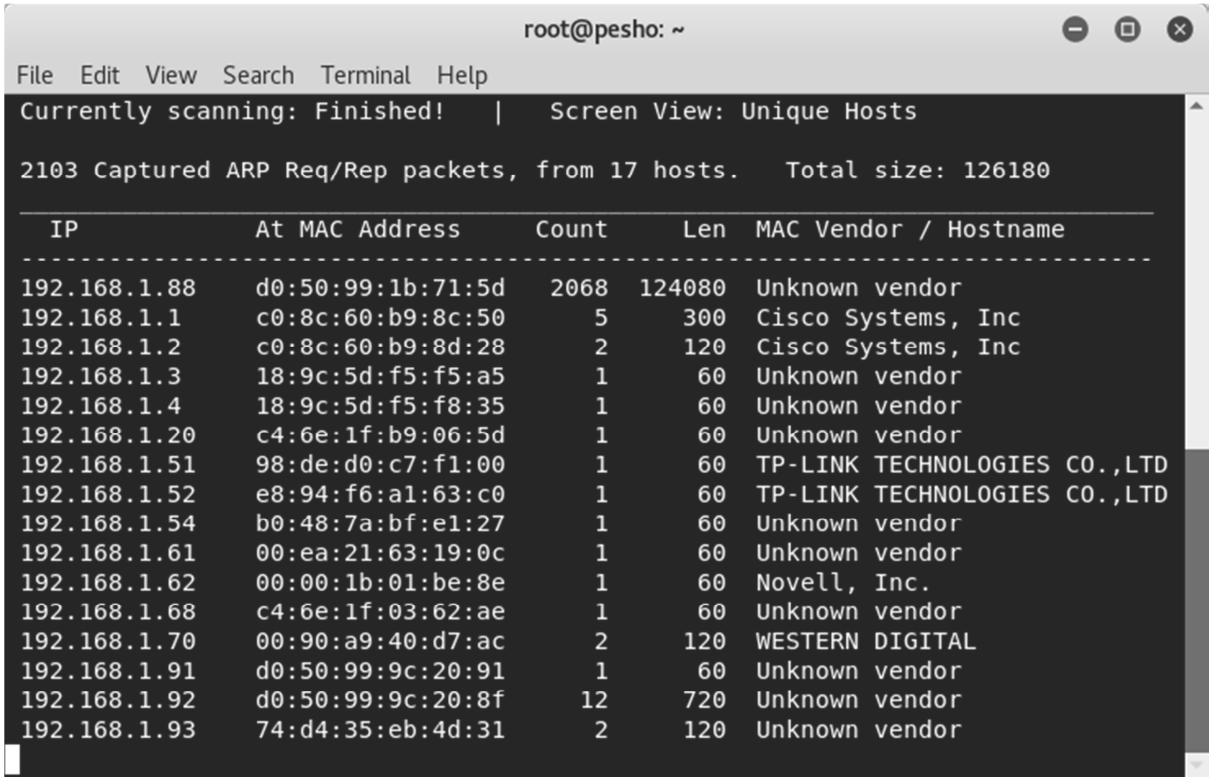

Figure 1: Scanning for network states

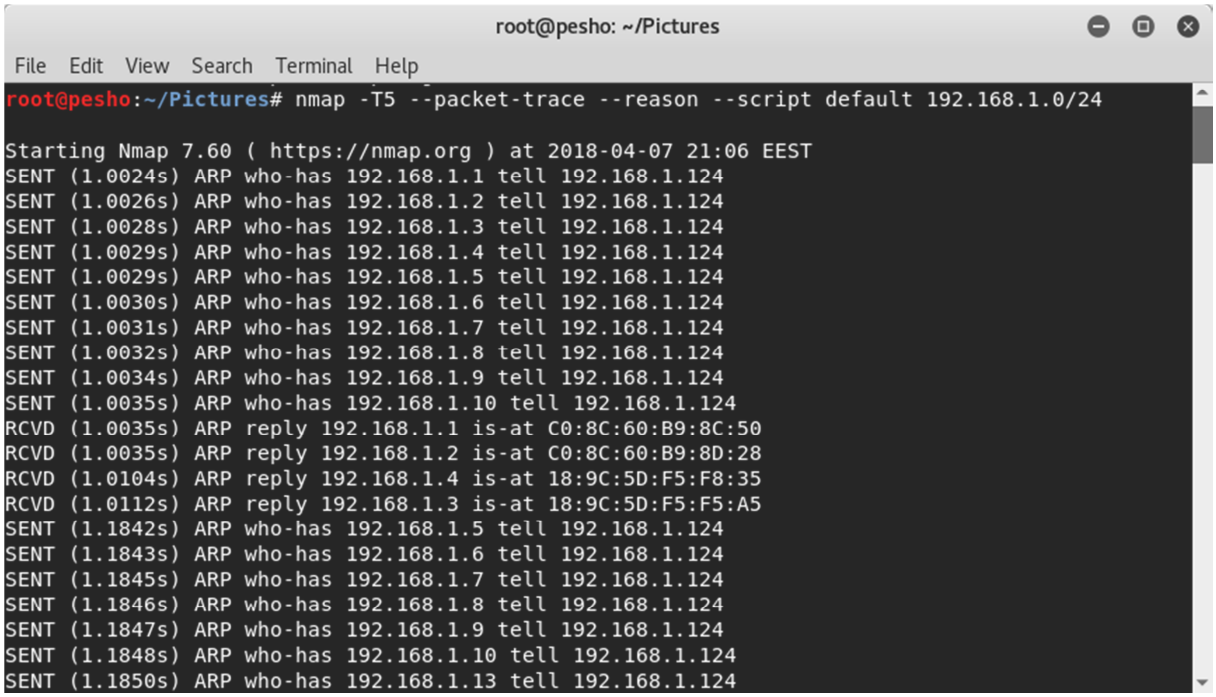

Figure 2: The successfully executed command “nmap -T5 --packet-trace --reason --script default 192.168.1.0/24”

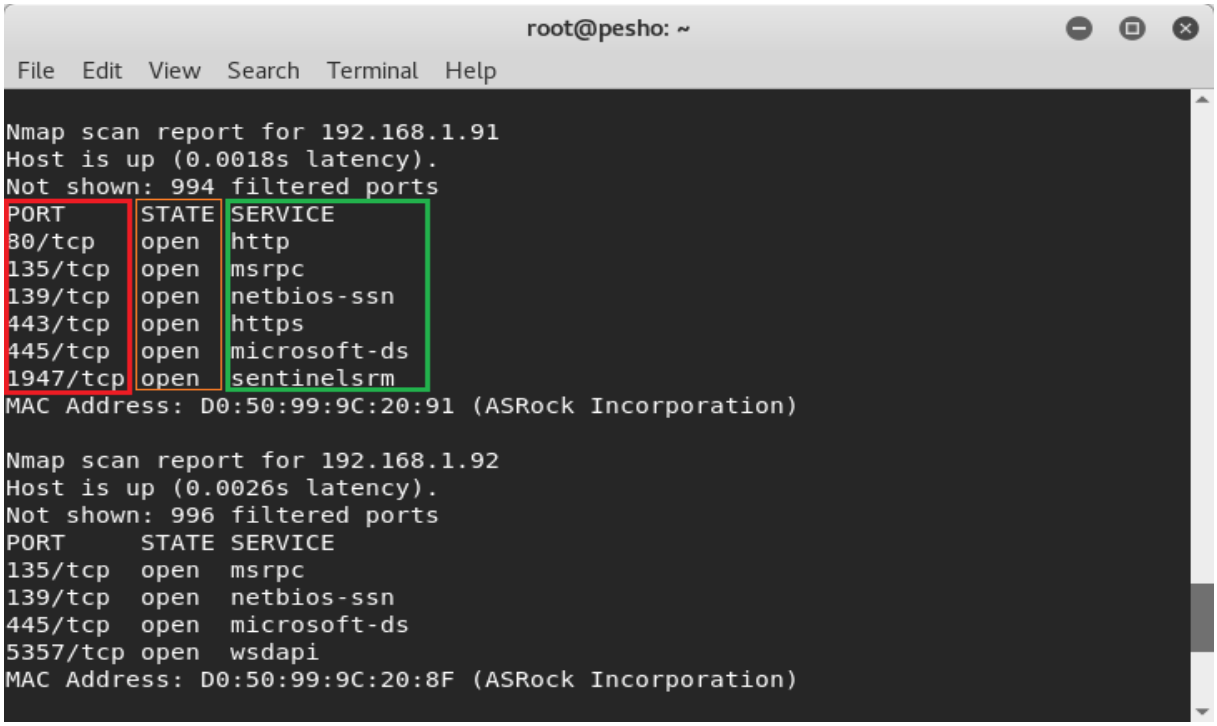

Figure 3: The results after the executed command “nmap -T5 --packet-trace --reason --ip-options T 192.168.1.0/24”

The scanning time for vulnerabilities and ports plays important role for discovering the weaknesses in the selected victims. In this paper two different scanning commands were tested. The configuration of the tested computer was Intel Core I3-3225 CPU @ 3.30 GHz, RAM 16 GB with 64-bit operating system type on workstation machine. The

results are illustrated in the following figure 4 and 5. Thanks to the achieved results it was estimated that with command “nmap -T5 --ip-options T 192.168.1.0/24” was achieved high performance and efficiency in the process of detecting the vulnerabilities and weaknesses in the surveyed victims in academic institutions and government agencies.

The security officers of automated information systems and security networks administrators should also pay special attention to the digital data encryption and creation of modified algorithms for Steganalysis [9, 10, 11, 12, 14].

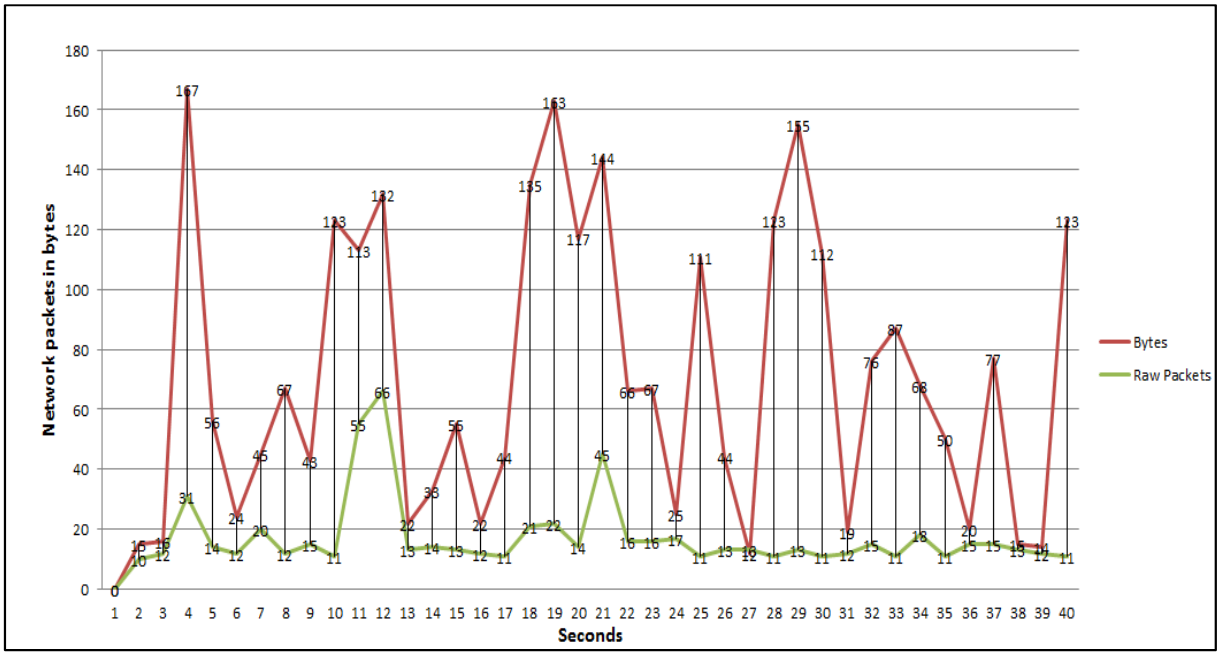

Figure 4: Scanning time performance with the executed command “nmap -T5 --packet-trace --reason --script default 192.168.1.0/24”

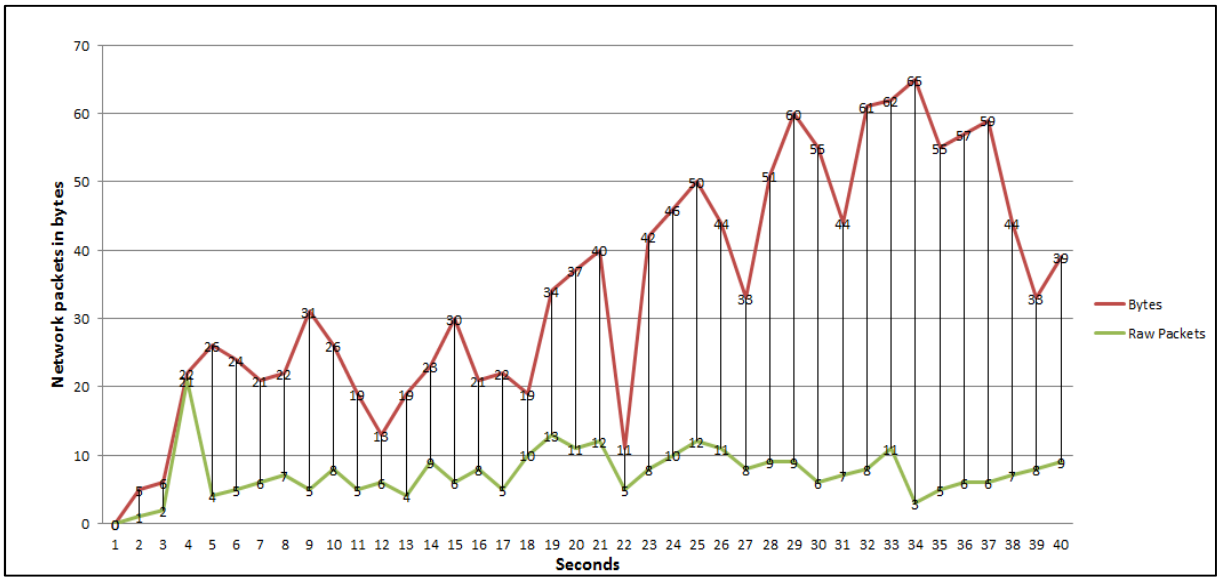

Figure 5: Scanning time performance with the executed command “nmap -T5 --ip-options T 192.168.1.0/24”

4. Conclusion

Thanks to the achieved results the security officers of automated information systems and security networks administrators mandatory must stop and block any ICMP requests. Another very important task is the implementation and configuration of stateful firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS). The security officers of automated information systems and security networks administrators may also must use other vulnerability scanners such as MBSA, Security Manager Plus, Shadow Security Scanner, Security Auditor's Research Assistant (SARA), Nsauditor Network Security Auditor in order to detect earlier the scanning cyber-attacks of the cyber-criminals.

Acknowledgments

The work is supported by the Scientific research fund of Konstantin Preslavsky University of Shumen under Grant No.: RD-08-144\08.02.2018.

References

[1] Boyanov, P., Hristov, H. 2018. Implementation of network enumeration cyber-attacks and defense the computer resources of the local and wide area networks, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), 2018.

[2] Boyanov, P. 2014. 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.

[3] Boyanov, P. 2013. "A taxonomy of the cyber attacks", a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), ISSN 1314-6289, Vol.3, 2013, pp. 114 – 124.

[4] Boyanov, P., Zhaneta, T. 2013. "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.

[5] Boyanov, P. 2013. A sophisticated information gathering and security auditing of computer and network resources using the cross-platform portscanner Zenmap, International Conference on Bionics and Prosthetics, Biomechanics and Mechanics, Mechatronics and Robotics (ICBBM 2013), Riga - Latvia, LABPOTO - Latvia, ISBN 978-9934-8409-0-6, Volume 9, June 17 - 21, 2013, pp. 154-157.

[6] Dosev N. Y. 2017. Sazdavane na sklad ot danni za opredelyane na riska za informatsionnata sigurnost na korporatsiyata", Nauchna konferentsia s mezhdunarodno uchastie na tema „Kibersigurnostta v informatsionnoto obshtestvo”, Fakultet "A, PVO i KIS", Shumen.

[7] Dosev N. Y. 2014. Nepravitelstveniyat sektor i natsionalnata sigurnost“, Treta mezhdunarodna nauchna konferentsia –„Nauka, obrazovanie, inovatsii“, posvetena na 145 godishninata na BAN i 35 godishninata ot kosmicheskia polet na Georgi Ivanov, 21-23-05. Shumen.

[8] Hristov, Hr., Boyanov, P., Trifonov, T. 2014. Approaches to identify vulnerabilities in the security system of the social organization and computer resources, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 5, pp. 101-107.

[9] Kordov, K., Bonchev, L. 2017. Using circle map for audio encryption algorithm, Mathematical and Software Engineering, 3(2), 183-189.

[10] Nachev, A., Zhelezov, St., 2013. Assessing the efficiency of information protection systems in the computer systems and networks. Informatsionnые tehnologii i bezopasnosty, Zhurnal Akad. nauk Ukrainы., Spets. vipusk, Kiev, Str. 79-86.

[11] Stanev St., Szczypiorski Krzysztof. 2016. 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, DOI: 10.1515/eletel-2016-0043.

[12] Stoyanov, B., Zhelezov, S., Kordov, K. 2016. Least Significant Bit Image Steganography Algorithm Based on Chaotic Rotation Equations, Comptes rendus de l’Academie bulgare des Sciences, Vol. 69, No. 7, 845-850, ISSN 2367-5535.

[13] Vasileva, R. 2015. „Analiz na sastoyanieto na zashtita pri bedstvia v Bulgaria“, NS s mezhdunarodno uchastie "Kursantite i studentite na morskoto uchilishte i naukata", VVMU “N. Y. Vaptsarov", Varna, 26-27 mart 2015 g.

[14] Zhelezov, St. 2015. Modified Algorithm for Steganalysis, Mathematical and Software Engineering, 1(2), 31-36.