Journal scientific and applied research, vol. 5, 2014
Association Scientific and Applied Research
International Journal

Original Contribution

ISSN 1314-6289

USING THE COLASOFT CAPSA NETWORK ANALYZER TO DIAGNOSE, PINPOINT AND DETECT A VIRIETY OF MALICIOUS CYBER-ATTACKS AND TO IMPROVE THE VULNERABILITIES FOR A SOHO NETWORK

Petar Boyanov

KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN,
SHUMEN 9712, 115, UNIVERSITETSKA STR,
E-MAIL: peshoaikido@abv.bg

Abstract: *In this paper a high-level analyzing for different malicious attacks is made. Thanks to the real-time network analyzer Colasoft Capsa some applications problems and vulnerabilities have been detected and thereby this action ensures a protection for the hosts in the SOHO network. Nowadays it is desirable that many cyber-security professionals and network managers to use Colasoft Capsa in order to detect and protect the computer and network systems against malicious cyber-attacks.*

Key words: *Cyber-attacks, Network analyzing, SOHO, Vulnerability.*

1. Introduction

The cyber-attacks cause irreparable damages on computer network systems. Therefore it is necessary to be analyzed and scanned the hosts against different malicious cyber-attacks and troubleshooting in the specified network.

Previous technical papers illustrated only common features and characteristics of the network analyzer Colasoft Capsa. In this paper some comprehensive network analyzes for different application problems and cyber-attacks in one SOHO (Small Office/Home Office) Network are made in order to be detected some malicious cyber-attacks and to be provided high-level security mechanisms for the hosts. The achieved result in this paper shows that each network hides a lot of malicious cyber-attacks and each network security expert must continuously to analyze and monitor the traffic information in the determined network.

This paper is structured as follows. First, in section 2, a comparative analyzing of the software product Colasoft Capsa is made. After that, in section 3, a sophisticated implementation of Capsa against different malicious cyber-attacks in determined SOHO network (79.100.128.0/21) 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] the connection and traffic between each host in the determined network by Asrodia and Patel is shown. The Calculation of traffic volume generated by web users is made by Dunaytsev, Krendzel, Koucheryavy, Harju [2]. In [3] the software product Colasoft Capsa 6.0 to filter IPV4 packets by [3] Kahya-Özyirmidokuz, Gezer and Ciflikli is used. In [4] a simple implementation with the packet analyzer Colasoft Capsa by Kumar and Arumugam is demonstrated. In [5] a common characteristic of the software product Capsa by Singh G. and Singh A. is made. In [6] Capsa with other software products by Venkatramulu and Rao is compared. In [7] the cyber-attacks that Capsa can detect by Zaefferer, Inanir and Karanatsios are presented.

3. Experiment

This experiment in a SOHO (Small Office/Home office) network is made. The local subnet is 79.100.128.0/21. This means that this network consists of 2048 hosts. In this network a DHCP (Dynamic Host Configuration Protocol) is activated in order to receive each host automatically IP (Internet Protocol), network mask, default route address and DNS server address. The investigated host uses the following IP address 79.100.129.167/21 and used operating system is Microsoft Windows 7 Ultimate.

The Colasoft Capsa is a sophisticated network analyzer software tool. The key features in this tool are [1], [2], [3], [4], [5]:

- Sophisticated protocol analyzing.
- Real-time packets capturing for wired and wireless networks.
- Providing a network statistics for the whole network.
- Making a summary report.
- Detection for a Worm - cyber-attack.
- Detection of Dos Attacking.
- Detection of ARP attack.
- TCP port scanning.
- Detection of Suspicious conversation.
- Diagnosis of security analysis.
- The used protocols.
- Detection of physical conversation.
- Detection of IP conversation.
- Detection of TCP conversation.
- Detection of UDP conversation.
- Making an entire matrix map.
- Making Global log, DNS log, Email log, FTP log, HTTP log and etc.

The used software tool in this paper has 15-days trial license. The version of this product is 7.7.1 and the build is 3076 [4,], [5], [6].

The achieved diagnosis after the made investigation illustrates that network 79.100.128.0/21 has been attacked via ARP cyber-attack. This is shown on fig. 1.

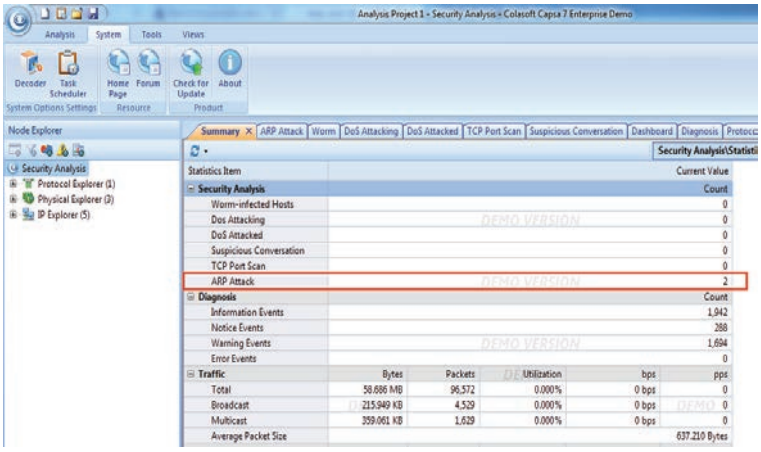

Fig. 1. The achieved diagnosis after the made investigation

The attacked hosts are shown on fig. 2.

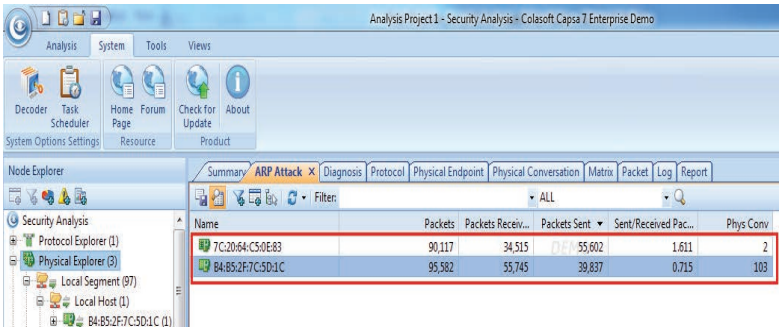

Fig. 2. The attacked hosts

The first host has 7C:20:64:C5:0E:83 MAC address and the second host has B4:B5:2F:7C:5D:1C MAC address. The MAC address B4:B5:2F:7C:5D:1C belongs to host with IP address 79.100.129.167.

On fig. 3 The all diagnosis information about host with the MAC address B4:B5:2F:7C:5D:1C is shown.

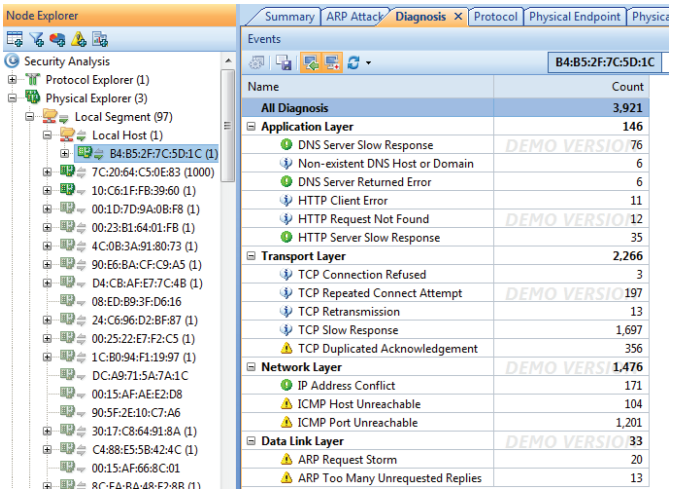

Fig. 3. The all diagnosis information about host with MAC address B4:B5:2F:7C:5D:1C

This diagnosis information shows the following items:

- DNS Server Slow Response – 76.
- Non-existent DNS Host or Domain -6.
- DNS Server Returned Error – 6.
- HTTP Client Error – 11.
- HTTP Request Not Found – 12.
- HTTP Server Slow Response – 35.
- TCP Connection Refused – 3
- TCP Repeated Connect Attempt – 197.
- TCP Retransmission – 13.
- TCP Slow Response – 1697.
- TCP Duplicated Acknowledgement – 356.
- IP Address Conflict – 171.
- ICMP Host Unreachable – 104.
- ICMP Port Unreachable – 1201.
- ARP Request Storm – 20.
- ARP Too Many Unrequested Replies – 13.

In its essence the ARP (Address Resolution Protocol) is responsible for the converting a specific IP address to a physical address such as MAC (Media Access Control) address. Therefore by the ARP attack the cyber-criminal has the ability to send spurious ARP messages in the determined Local Area Network. The underlying purpose of the cyber-criminal is to associate him MAC (Physical) address with the IP address of another host such as intelligent switch or router. After the established session the cyber-criminal can quite easily either interrupt or transmute the whole network traffic [1], [6], [7].

On fig. 4 the physical conversation between the compromised host (B4:B5:2F:7C:5D:1C) and the attacking hosts is shown.

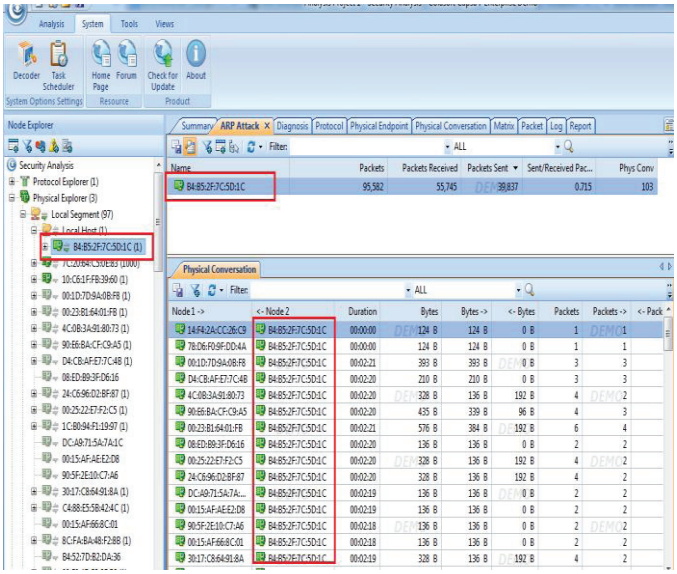

Fig. 4. The physical conversation between the compromised host (B4:B5:2F:7C:5D:1C) and the attacking hosts

On fig. 5 the Top100 IPv4 conversation of host 79.100.129.167 is shown.

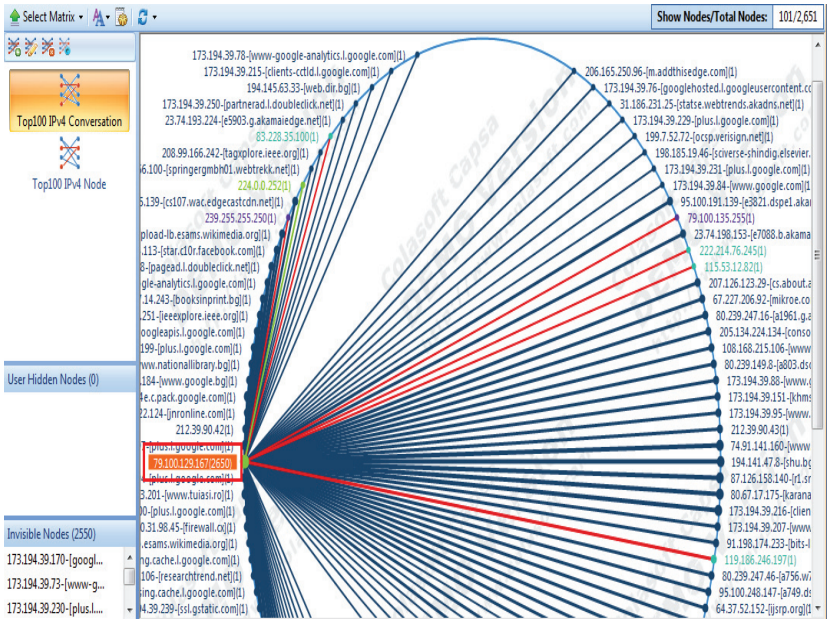

Fig. 5. The Top100 IPv4 conversation

The global log of host 79.100.129.167 on fig. 6 is shown.

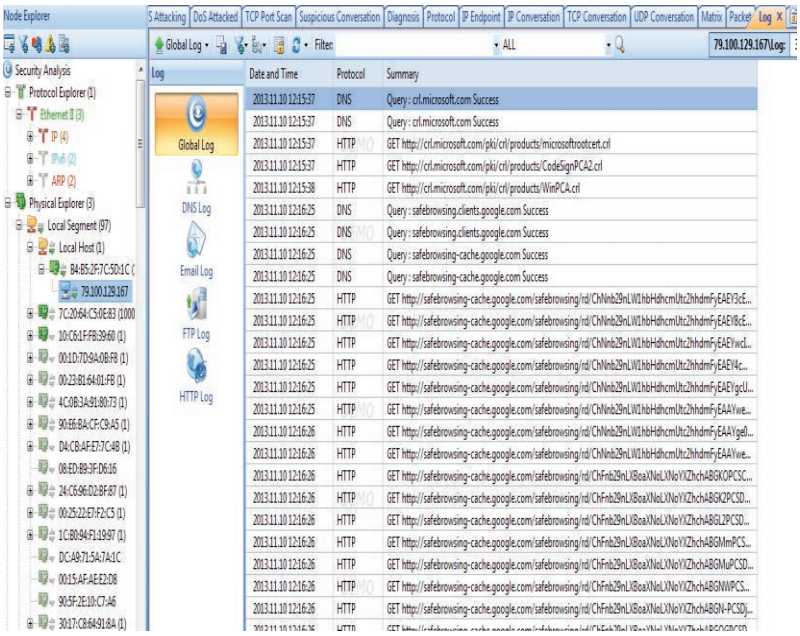

Fig. 6. The global log of host 79.100.129.167

4. Results

On fig. 7 the top application protocols by bytes is illustrated.

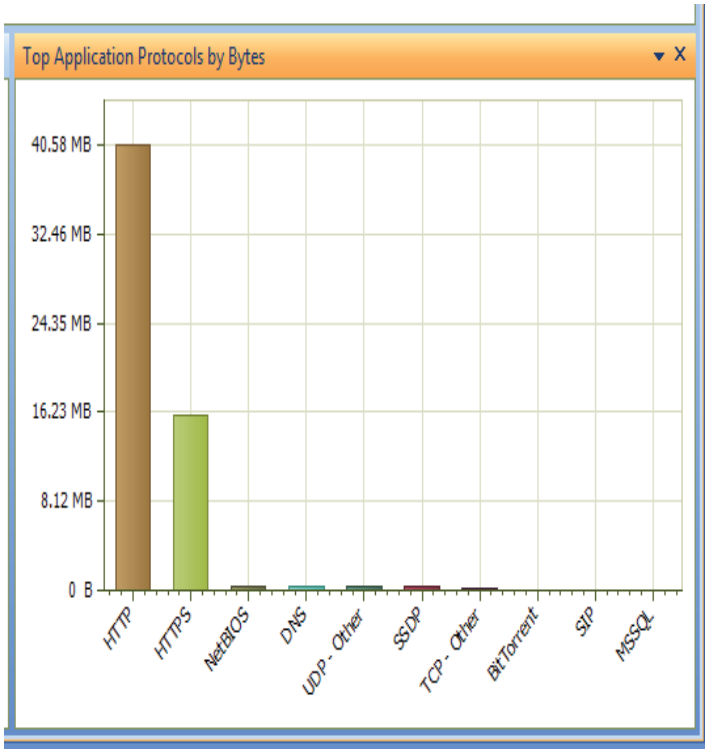

Fig. 7. The top application protocols by bytes

On fig. 8 the total traffic by bytes is shown.

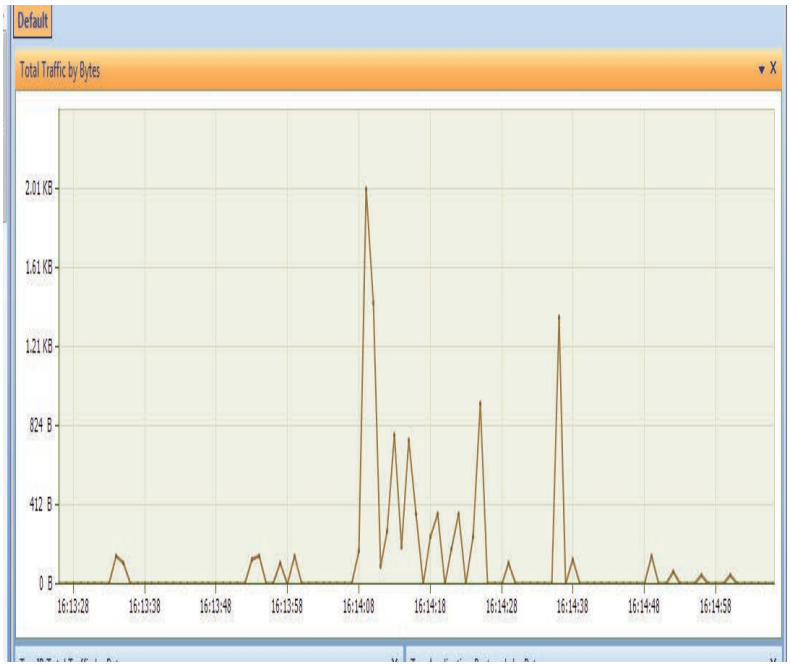

Fig. 8. The total traffic by bytes is shown

Thanks to the software Colasoft Capsa each network security expert has the ability to analyze, monitor and scan a determined SOHO network especially for network cyber-attacks such as ARP spoofing attacks, Worn attacks, DoS attacks, Suspicious conversation attacks and etc.

5. Conclusion

In this paper a high-level scanning and analyzing of a determined SOHO network (79.100.128.0/21) is made. Thanks to the achieved results each network security expert and IT security manager has the ability to detect different malicious cyber-attacks such as ARP spoofing attacks, DoS attacks, DDoS attacks, Worm attacks and etc. After the detection of a specific cyber-attack the network security expert must interrupt the internet connection and to close all open ports. It is recommended to be installed IDS (Intrusion Detection System) and IPS (Intrusion Prevent System) control points before and after the router side in the selected network. These systems are designed to detect various malicious cyber-attacks and to prevent their future executions into the target host.

Acknowledgements

This paper is supported by the Project BG051PO00l-3.3.06-0003 “Building and steady development of PhD students, post-PhD and young scientists in the areas of the natural, technical and mathematical sciences”. The Project is real-

ized by the financial support of the Operative Program "Development of the human resources" of the European social found of the European Union.

References:

[1] Asrodia P., & Patel H., Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis, International Journal of Electrical, Electronics and Computer Engineering 1(1): 55-58(2012)

[2] Dunaytsev, R. A., Krendzel A. V., Koucheryavy Y. A., & Harju J. J., Estimation of web traffic generated by users in home networks, Proceedings of the eighth IASTED IMSA', Kauai, Hawaii. Retrieved from/http://www.cs.tut.fi/tlt/npg/icefin/documents/Hawaii-427-141_Final_Manuscript. pdfS, 2004

[3] Kahya-Özyirmidokuz E., Gezer A., & Ciflikli C., Characterization of Network Traffic Data: A Data Preprocessing and Data Mining Application, In DATA ANALYTICS 2012, The First International Conference on Data Analytics, 2012, September, pp. 18-23

[4] Kumar P. S., & Arumugam S., Establishing a valuable method of packet capture and packet analyzer tools in firewall, International Journal of Research Studies in Computing, 2012 April, Volume 1 Number 1, 11-20

[5] Singh G., & Singh A., Campus Network Security Policies: Problems And Its Solutions, International Journal of Innovative Research and Development, June, 2013, Vol 2 Issue 6, pp.294-306

[6] Venkatramulu S., & Rao C. G., Various Solutions for Address Resolution Protocol Spoofing Attacks, International Journal of Scientific and Research Publications, Volume 3, Issue 7, July 2013

[7] Zaefferer M., Inanir Y. S., & Karanatsios T., Intrusion Detection, University of Applied Sciences Cologne, Faculty for Informatics and Engineering, Gummersbach, February 2012