

Original Contribution

Journal scientific and applied research, vol. 6, 2014 Association Scientific and Applied Research International Journal

ISSN 1314-6289

USING A SPECIALIZED SOFTWARE FOR COMPREHENSIVE MONITORING THE SUSPICIOUS STATES IN COMPUTER NETWORKS

Petar Boyanov

DEPARTMENT OF COMMUNICATION AND COMPUTER TECHNOLOGY, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712, 115, UNIVERSITETSKA STR, E-mail: <u>peshoaikido@abv.bg</u>

Abstract: In this paper a comprehensive scanning and monitoring the suspicious states in determined computer networks is made. Most of the computer and network problems with many vulnerabilities are connected. Therefore it is advisable to scan the entire computer network in order to detect weaknesses and accordingly be taken precautions Thanks to the many malicious users will not be able to penetrate in the relevant computer network and to gain access to computer resources.

Key words: Computer and network security, cyber-attacks, Monitoring, Penetration, Scanning, Sensors, Vulnerabilities, Windows 7.

1. Introduction

Each computer network must be repeatedly scanned and monitored with specialized application software products. Many of the cyber-criminals and malicious users use the vulnerabilities in these computer network systems in order to gain an unauthorized access and therefore to compromise confidential user information. This paper is structured as follows. First, in section 2, different measurement techniques of network scanning and monitoring are made. After that, in section 3, class C network (192.168.0.0/24) for vulnerabilities, errors and problems 24) is scanned and monitored. The achieved results are presented in section 4. The final conclusions and recommendations are made in section 5.

2. Related work

In [2] a HTTP traffic measurements on determined networks by Vladimir Deart, Vladimir Mankov and Alexander Pilugin, is made. In [5] autonomous malicious activity inspector - AMAI by [5] Umar Manzoor, Samia Nefti and

Yacine Rezgui is presented and used. In [7] the software PRTG Network Monitor by Paessler, A. G. is explained. In [10] network traffic monitoring and analysis tools by Chakchai SO-IN are presented and classified. In [12] network monitoring based on flow measurement techniques by Michiel Uithol is performed.

3. Experiment

The experiment in specialized university computer lab is made. The network ID of this LAN is 192.168.0.0/24. The used software is PRTG network monitor freeware version. Initially was necessary to configure the software product. The SSL encryption connection has been made. After that credentials for SNMP (Simple Network Management Protocol) [12] based network devices was chosen. Most of the network devices like switches, routers, multilayer switches and firewalls support this protocol for scanning and monitoring the determined network. The version v2c and SNMP [9],[10],[11] port 161 were selected. The DNS server addresses were also entered. A network class C (192.168.0.0/24) was configured. The IP address range has been started from 1 and ended at 254. The following experiments only with education intend and purposes are made. The Microsoft Windows 7 Enterprise SP1 operating system in the scanning host has been used. On fig. 1 the overview of the discovered network is shown.

	vork Monitor Jevices Libraries Sensors	Alarms Maps Reports	Logs ToDos Setup			D: PAES: Φ ? ৩ Ø Search.
evices		manny mapy nepond	10005 5000			New Log Entries 43 ToDos 5 12 8
up R	loot					Group Details
rview	2 days 30 days 365 days	Alarms Log Ø Man	agement 🎤 Settings 🗛	Notifications 📾 🔳		Use the tab controls to vi various data of this group
B 2	V 10 V 10 V 18				o 💿 🔘 🗩 Sear	as well as edit the group'
						Geo Map settings
R						Auto-Discovery
	Local probe				The fastest way to create	
	I IIII Probe Device	Core Health 100 %	Probe Health	System Health	Dick Free	sensors for your network to use PRTG's automatic
		Ralink RT3290 802 11bgn Wi-Fi A	Teredo Tunneling Pseudo-Inte	t.		device discovery function. Simply click on 'Add
E	🗟 1st group	-				Click here to enable or his Auto-Discovery Group' to
	+ Add Device					
						Click here to enable or hic start.
E	Group 1					2 days Help: Auto-Discovery
Ε		PINS 1	DNS 1			2 days 100 - Provide of mustart. Help: Auto-Discovery
Ε	Group 1 Group	0 maec	6 msec	Disk Free 1	11 Memory 1	2 days 100 - # 50 - With 977 minutes and 1
E	Group 1	asem 0	6 maac	11 Disk Free 1 11 Local Area Connection* 37	11 Memory 1 11 Rainics 872209 602 118gr Wi-Fi A.	2 days 100 - # 50 - 0 - 100 - 10
E	Group 1 m 192168.0.1 pcworkGROUP	0 maec	6 msec CPU load 1 14%			2 days 100 - # 50 - 0 - 100 - 10
Ε	Group 1 192168.0.1 By PESHOSAN- PC.WORKGROUP (Peshosan-PC)	0 masc PtNG 2 0 masc III Pagefie Utage 1	6 mses CPU Lead 1 14 % WMI Uptime 1	Local Area Connection* 37		2 days Help: Auto-Discovery 100 Remote Site Monitoring # 50 With PRTG you can monit 50 Remote Site Monitoring with PRTG you can monit Runubic probes. PRIG 50 State 6 State 7 Runubic give to can ad automatically. You can ad automatically. You can ad automatically.
E	Group 1 900 192168.0.1 987 PESHOSAN- PC.WORKGROUP (Pethosan-PC) [Windows] 900 PC-ZAEMNA1	Omsec Paysis Pagefile Usage 1 Teredo Tunneling Pseudo-Unterf PRVG 3	6 msec C CPU Load 1 14% WML Uptime 1 Windows Defender RDP (Remote Desistop) 2	Local Area Connection* 37		2 days Help: Auto-Discovery 100 Feat # 50 Feat 0 Feat 100
	Group 1 92168.0.1 97295405AN- PC-WORKGROUP (Pethosan-PC) (Windows) 972742 97274 972742 97274 9774 97	2 misec PING 2 Payelie Usage 1 Pagefile Usage 1 Teredo Tunneling Pseudo-Interf	6 msec CPU load 1 14% 11 WM Uptime 1 11 Windows Defender	Local Area Connection* 37		2 days 100 # 50 100 # 50 100 100 100 100 100 100 100 1
	Group 1 192168.0.1 PENDSAN PCWORKGROUP (Pethosan-PQ Windows) PC-ZAEMINA1 PC-ZAEMINA1 SHU-LIB Internet Connection	Price P	6 msec C CPU Load 1 14% WML Uptime 1 Windows Defender RDP (Remote Desistop) 2	Local Area Connection* 37		2 days Help: Auto-Discovery 100 Remote Site Monitoring 100 With PRIG you can monit your network using multiple probes. PRIG Alams (*) CPU Load Index (%) 100 CPU Load Index (%)
	Group 1 92168.0.1 97295405AN- PC-WORKGROUP (Pethosan-PC) (Windows) 972742 97274 972742 97274 9774 97	Price P	6 msec C CPU Load 1 14% WML Uptime 1 Windows Defender RDP (Remote Desistop) 2	Local Area Connection* 37		2 days Help: Auto Discovery 2 days Help: Auto Discovery 4 50 With PRTG you can monit your network using the comparison of the comparison automatrally, you can ad automatrally to us can automatrally to the the monitor remote sites and monitor remote sites and to us can automatrally to us can automatra

Fig. 1. An overview of the discovered network

The figure has shown that there are several subgroup of the root mainframe.

The Local probe group has showed that there are two important alarm notifications. The first sensor was Disk free and his status was in down state. The message was "7% (Free Space D:) is below the error limit of 10%. The second sensor message was Teredo Tunneling Pseudo-Inferface and his status was also in down state [2],[5],[10]. The warning message was "Could not log in using the specified credentials. Please make sure they are not only valid for the target system, but for the probe system as well. (Performance Counter error 0xB0000004).

The group 1 show has presented several important results as well.

The ping and DNS probe for host with IP address 192.168.0.1 were successfully made. The host PESHOSAN-PC.WORKGROUP (Peshosan-PC) had 2 successfully sensors for PING 2 and CPU Load 1, but at the same time had several sensors with warning states. These sensors were:

- Disk Free 1;
- Memory 1;
- Pagefile Usage 1;
- WMI Uptime 1;
- Local Area Connection* 37 [2], [4];
- Windows Defender;
- RDP (Remote Desktop) 1 and etc.

The other discovered hosts were PC-ZAEMNA1 and SHU-LIB.

The Internet connection group has shown only two sub-domain addresses - fmi.shu-bg.net and ns.shu-bg.net.

4. Results.

Thanks to the achieved scan and monitor of the selected local area network there has been found some flaws, errors and vulnerabilities. It is recommended and important the appropriate configurations be made. On fig.2 several sensor graphs are shown.



Fig. 2. Several sensor graphs

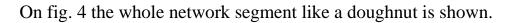
On fig. 3 the behavior of the probe device - Ralink RT3290 802.11bgn Wi-Fi Adapter is shown.

	aries Sensors	Alarms Ma		Logs	ToDos	Setu	ıp								
) Devices) Local probe 💌) Probe Device 💌)	Ralink RT3290 802.118	g_ ₩	_	_	_	_	_	_	_	_			_	New
	Ralink RT3290 802.11bgn Wi-Fi Adapter 🗖 🖉														
	Max: 1,140,743 kbit/s - 70,000,000														
1,000,000 -															
												- 60,000,000			
800,000 -												- 50,000,000			
												- 40,000,000 <u>vi</u>			
면 000,000 - 단 000,000 -									1			¥ - 30,000,000			
400,000 -									-			30,000,000			
												- 20,000,000			
200,000 -												- 10,000,000			
0			-	Min	: 1 kbit/s	_		_			_	- 0			
5 (C. 1)	- Mq - Mq	- Mq	MA	ΣΣ	Md	M	N N	- Md	ž	M M M	- Mo	1 0			
20	55 00 10	3:15 F 3:20 F 3:25 F	3:30 PM 3:35 PM 3:40 PM	3:50 PM	3:55 PM 4:00 PM	4:05 PM	4:15 PM	4:20 F	MH (7:+	4:30 PM 4:35 PM	4:40 PM 4:45 PM				
RTG Network Monitor 13.1.2.1462	й й й й 		~ ~ ~ ~ !	m m	ω 4	4-	4 4	4 .	+	4 4	4 4	7/30/2014 4:47:40	PM		
Downtime (%)	🗹 Total (kbit/	(s) 🗹 Tr	affic in (kbit/s)	2	Traffic ou	t (kbit/	(s) 🔽	Packets	(#/s	;)					
nsor Data															
ate Time	Total (volume)	Total (speed)	Traffic in (volum	ne) Tra	ffic in (sp	eed) T	raffic ou	it (volum	e) T	raffic ou	t (speed)	Packets (volume)	Packets (speed)	Downtime (Coverage
ums (of 120 values)	24,544,753 KByte		11,983,064 KB	yte			12,56	1,689 KBy	te			12,884,239,129 #			
verages (of 120 values)) 204,540 KByte	27,938 kbit/s	99,859 KB	yte	13,640 k	bit/s	10	4,681 KBy	te	14,2	298 kbit/s	107,368,659 #	1,790,194 #/s	0 %	100 %
← 1 to 50 of 120 → →) (⁰													▼ Item C	ount
ate Time 🔺	Total (volume)	Total (speed)	Traffic in (volur	ne) Tra	ffic in (sp	eed) T	raffic ou	it (volum	e) T	raffic ou	t (speed)	Packets (volume)	Packets (speed)	Downtime (Coverage
10/2014 4:47:40 PM	43 KByte	6 kbit/s	31 KB	yte	4 k	bit/s		13 KBy	te		2 kbit/s	373 #	6 #/s	0 %	100 %
L0/2014 4:46:40 PM	40 KByte	5 kbit/s	27 KB	yte	4 k	bit/s		13 KBy	te		2 kbit/s	433 #	7 #/s	0 %	100 %
/10/2014 4:45:40 PM	55 KByte	e 8 kbit/s	36 KB	yte	5 k	bit/s		19 KB)	te		3 kbit/s	621 #	10 #/s	0 %	100 %

Fig. 3. The behavior of the probe device - Ralink RT3290 802.11bgn Wi-Fi Adapter

This graph had the following important items:

- Date Time;
- Total (volume);
- Total (speed);
- Traffic in (volume) [3], [6], [8];
- Traffic in (speed);
- Traffic out (volume);
- Traffic out (speed);
- Packets (volume);
- Packets (speed) [9], [11];
- Downtime;
- Coverage and etc.



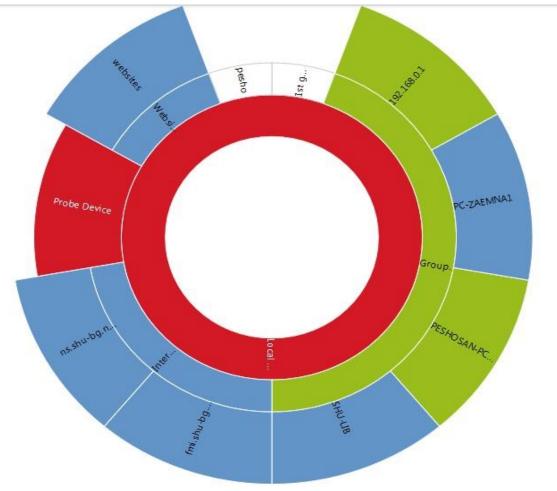


Fig. 4. The whole network segment

In the core of this doughnut it could be seen that the local probe is in red color and means that the system administrator or security-professionals must take measures to fix the following problems and therefore to reduce the weaknesses in the selected computer network.

5. Conclusion

In this paper a comprehensive scanning and monitoring the suspicious states in determined computer networks is made. Thanks to the achieved results for the selected network 192.168.0.0/24 the system administrator and IT specialists must take actions and to fix the problems and to figure out specialized plans that will protect the entire computer network system from various malicious cyber-attacks. The daily scanning and testing for weaknesses is the best solution for the correct and stable operation of the system.

Acknowledgements

This paper is supported by the Project BG051PO001-3.3.06-0003 "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 realized by the financial support of the Operative Program "Development of the human resources" of the European social found of the European Union.

References:

- [1] Branam, Michael, et al. Methods, systems, and computer program products for providing network convergence of applications and devices. U.S. Patent Application 11/537,708, 2006.
- [2] Deart, Vladimir; Mankov, Vladimir; Pilugin, Alexander. HTTP Traffic Measurements on Access Networks, Analysis of Results and Simulation. In: Smart Spaces and Next Generation Wired/Wireless Networking. Springer Berlin Heidelberg, 2009. p. 180-190.
- [3] Gold, Steve. Hacking on the hoof. Engineering & Technology, 2012, 7.3: 80-83.
- [4] Manzoor, Umar; Nefti, Samia; Rezgui, Yacine. Categorization of malicious behaviors using ontology-based cognitive agents. Data & Knowledge Engineering, 2013, 85: 40-56.
- [5] Manzoor, Umar; Nefti, Samia; Rezgui, Yacine. Autonomous malicious activity inspector–AMAI. In: Natural Language Processing and Information Systems. Springer Berlin Heidelberg, 2010. p. 204-215.
- [6] Nualmuenwai, Paramet; Prommak, Chutima. On the Analysis of IP Traffic Distribution in the Network of Suranaree University of Technology. In: Conf. WASET, Thailand. 2011. p. 362-365.

- [7] Paessler, A. G. the Network Monitoring Company, PRTG Network Monitor.
- [8] Paessler, Dirk. Server Virtualization and Network Management. Database and Network Journal, 2008, 38.5: 13.
- [9] Park, Daihee, et al. NetCube: a comprehensive network traffic analysis model based on multidimensional OLAP data cube. International Journal of Network Management, 2013, 23.2: 101-118.
- [10] SO-IN, Chakchai. A Survey of Network Traffic Monitoring and Analysis Tools. Cse 576m computer system analysis project, Washington University in St. Louis, 2009.
- [11] Song, Yuqian, et al. Towards a framework to support novice users in understanding and monitoring of Home Area Networks. In: Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on. IEEE, 2012. p. 82-87.
- [12] Uithol, Michiel, et al. Section 2: Network monitoring based on flow measurement techniques. SURFnet Research on Networking (RON) Project.