Network Security Scoring

Conference Paper · January 2017

DOI: 10.1109/ICSC.2017.86

CITATIONS
6

READS
423

2 authors:

Sami Kacar
KTO Karatay University
1 PUBLICATION **6** CITATIONS
SEE PROFILE

Kasim Oztoprak
Konya Food and Agriculture University
30 PUBLICATIONS **121** CITATIONS
SEE PROFILE

Network Security Scoring

Mustafa Sami Kaçar
Department of Computer Engineering
KTO Karatay University
Konya, Turkey 42020
Email: msami.kacar@karatay.edu.tr

Kasım Öztoprak
Department of Computer Engineering
KTO Karatay University
Konya, Turkey 42020
Email: kasim.oztoprak@karatay.edu.tr

***Abstract*—Network Security is one of the most critical issues of establishments like universities, public and private enterprises which have significant role on operations and security of a state. These enterprises use Internet to share and keep official information, and to make their corporate operations. A cyber attack that targeted such establishments networks may cause a great loss. Therefore, networks of these enterprises ought to be protected on a high level security. In this paper, a system is offered which is able to investigate networks of enterprises and ranking their network by predefined parameters. Moreover Network Security Simulator is also offered to implement the system.**

***Keywords*—network security; security scoring; Network user analyzing; Network component analyzing**

I. Introduction

Universities, public and private enterprises and their networks security have critical importance on national security. These organizations own crucial data of a state or citizens of that state. They communicate with external world via Internet that is implemented on a local network. That makes networks critical points to have a potential of external cyber attacks by malicious users and organizations.

It is of great convenience for people to get services online from enterprises. It also helps enterprises to reduce the process management encumbrance. Storing data on electronic environment has pretty good sides as it prevents the data loss and makes easier to share data with other enterprises. However, it may damage deeply if enterprises do not protect the confidential information of the state and people. Hence, enterprises ought to prevent their networks from all kinds of attacks.

War is not made only by human and modern weapon in this age. Today, cyber war is even the most hazardous threat for states. Internal or external enemies have talent to steal confidential information of enterprises and civilians. They may render unserviceable to institutions, and they may also create chaos by attacking critical points of the state, such as communication, health and infrastructure services. Due to such vital reasons, network security of enterprises is critically important. Organizations ought to keep pace with new security technologies. They should consider their network security vulnerabilities and take precaution for these vulnerabilities.

In this paper, a network security ranking system is offered. This ranking system produces a score by scoring security parameters of related network, and scoring of the users network usage that is extracted from users log files in the network. A network security simulator program is also offered to implement the network security ranking system. The rest of the paper is organized as indicated below. In section 2, concept of network security and related works are summed up. Offered system is explained in section 3 and results are shown in section 4. Lastly paper is concluded in section 5.

II. Network Security

Potential of the Internet is increasing day by day depending on increasing of the usage and talents of the Internet. Beside of bringing innovations to daily life; it also threatens the world with the potential of misuse. Organizations ought to take precautions to cope with recent methods of the malicious users by recognizing their networks and implementing recent security technologies. In [1], author mentioned yesterday, today and future of the network security and clarified recent malicious methods and network security systems. As mentioned in that paper, particularly security of data networks, which involves Internet, is quite important.

Viruses, Worms, Trojans, Bots[1], IP Spoofing[2], Dos Attacks [2] and many other methods are used to threaten enterprises, civilians and Internet by the malevolent users. Even though these malicious methods and more are created wisely and competently, none of them are able to harm a network as much as users of the network. The authors in [3] determined the vulnerabilities of network security which is arisen by users in a network and they offered a system that trains the users in the network.

Anti Malware Tools, Firewalls[4], IDSs[5], VPNs[6] are instances of recent technologies that are beneficial tools to provide network security. Many of these technologies are no more optional for enterprises networks, they become a necessity. According to cyber network security company Symantec's published report , personal records of half billion people were stolen or lost in 2015[7]. Email Spam is rising every day. Also, mobile and web vulnerabilities are increasing. If inaccurate usage is also added in all these circumstances, it may be easier to understand why to use the network security technologies is a necessity.

As mentioned previous parts of this paper, analyzing users of a network is beneficial to protect network security. Most of the works are related to analyzing user activities of a specific website. The authors in [8] clarified why user analyzing in

[1] http://www.cisco.com/c/en/us/about/security-center/virus-differences.html
[2] http://www.cisco.com/c/en/us/about/press/Internet-protocol-journal/back-issues/table-contents-38/104-ip-spoofing.html

a network is used, and they indicated some tools which are used for that purpose, such as Google Analytics[3], AWStats[4] and Web Log Expert[5] . Moreover, as many others, programs like eWebLog[9], [10], NetIQ [11] are also freeware to use cleaning data, obtaining statistical inference. However, a study on scoring a network via scoring users by their Internet usage data which is found in log files of the network could not be found.

III. NETWORK SECURITY RATING SYSTEM - NESRAS ARCHITECTURE

Network management experts ought to know their managed network is safe enough to provide service or not. It is a vital necessity to see network security status. If the network is safe, experts may continue to work in order to maintain the system. Otherwise, if the network is in an emergency situation, experts ought to isolate the network, they may save the data before it is stolen, and recover the system before any leak occurs. Regular checking of a system is similar as a human's check up. If there is an unhealthy organ or tissue, doctor and patient ought to keep pace with the situation. The offered system in this paper is a kind of check-up system for networks. A network security simulator program is also offered to implement that check up system. NESRAS consists of two basic scoring steps. All scoring system is between 0 and 5. Higher score infers better conditions in network. At first, Internet usage activities are investigated by log files in the studied network. Users, who are connected to Internet via that network, are scored by the investigation, and a total score consists of users' scores. Secondly, network is scored and examined by some used or unused network security products. Later, both scores are added for scoring the network. The system produces a color with the obtained score. These are green, yellow, orange and red. Green means ideal network, there is no threat for institution. Stable network is represented by yellow which means experts of the network ought to check system but an emergency situation does not exist. While orange shows there are some problems in network, red implies that the network might be in a danger of attack. Intervals of colors according to scores are shown below:

- 0.0 - 1.5 => red
- 1.5 - 3.0 => orange
- 3.0 - 4.0 => yellow
- 4.0 - 5.0 => green

A. User Analytics

User anayltics, which was the first step of the system, was based on scoring the users in studied network. Dataset, which was used by author in [12], was used to analyze users. In that study, Internet category databases were used to create categorized and clean data from URL log files. Dataset included users; IP addresses, visited web pages, and categories of these visited web pages. DNS, operating system and web browser information were added to the original dataset by the statistics in[13], and a synthetic dataset, which was proper to the original dataset, was created to analyze the users. Network security simulator program took synthetic data as input in Comma-Separated Values(csv) file format.

1) Usage Analysis: At this stage, analyzing of users of the network who were connected to the Internet is clarified. Thus network experts would recognize user's activities in the network. They would see their managed network's vulnerabilities, and hazardous usages would also be distinguished.

Local IP addresses that was given in the studied network, web pages which were visited by these IP addresses, and categories of these web pages were located in dataset. With using local IP addresses, user privacy is preserved. Web pages were divided into 40 different categories in the dataset by Internet Category Engine (ICE) [12]. In this work, especially categories which could remind of danger were prioritized. Table 1 shows these potentially hazardous categories and scores of those categories. Scores of the hazardous categories were proposed as a hypothesis in this study.

TABLE I: HAZARDOUS CATEGORIES IN ICE AND SCORES OF THOSE CATEGORIES

Hazardous Categories	Scores
Malware/Virus	1
Malware/Virus	1
Potentially Dangerous	2
Pornography	1
Gambling	2
Unknown	1
Advertisements	2

Users were identified by IP addresses. Web pages and their categories were grouped by IP addresses. Thus, categories and web pages could be categorized for each user. Later, each user was scored by categories. Categories in Table 1 take the respective score in the table; other categories, which were not mentioned here, took default value which was '3'. Afterwards, category scores were summed and divided by total visits that were made by related IP address. For instance, if a user with IP address XYZ had visited 5 pages, and given that these pages were categorized by ICE as:

- ◇ 1 x Gambling
- ◇ 2 x Malware/Virus
- ◇ 2 x Search Engines

Usage Score of XYZ = ((1 x 2) + (2 x 1) + (2 x 3)) / 5

At the end of this part, each users' usage scores and overall usage score were produced. The largest rate impression on the user score was attained at this step.

2) Operating System Analysis: Operating systems (OS) of devices which users connected to the Internet over the studied network were examined by NESRAS considering their vulnerabilities. According to input dataset, operating systems of the users were scored, and these scores were added to the user score. Each operating system had different scores. Most popular operating systems and their scores are shown at Table 2. Scores were created in reference to [14] which was the data

[3]https://analytics.google.com
[4]http://www.awstats.org/
[5]https://www.weblogexpert.com/

regarding vulnerabilities in National Vulnerability Database (NVD)[6].

TABLE II: 6 MOST USED OPERATING SYSTEMS AND THEIR SYSTEM SCORES

Operating Systems	Scores
Linux	3,50
Windows 7	4,50
Android	3,30
IOS	4,00
Mac	OS X 3,70
Windows 10	4,30

3) Web Browser Analysis: At this step, web browsers of the users were examined. As mentioned by authors in [15], malicious users might carry out quite hazardous attacks to networks by web browsers' vulnerabilities. Scores were given to the web browsers, like operating systems analysis step, in reference to the [14]. Table 3 shows the most used web browsers and respective scores of these web browsers. Web browser scores influenced the user scores more than the operating system scores.

TABLE III: 5 MOST USED WEB BROWSERS AND THEIR SYSTEM SCORES

Web Browsers	Scores
Chrome	4,50
Internet Explorer	3,00
Firefox	5,00
Safari	3,50
Opera	4,00

4) DNS Analysis: DNSes are divided into 3 categories:

* Service Provider Assigned DNS
* Known servers DNS
* Unknown servers DNS

In this part, highest score '4.5' was given to the Service Provider DNSes. Because all responsibilities of DNS usage are on the Service Provider if a user prefers Service Provider Assigned DNS. Furthermore, Service Providers have to obey the law of located country, and assigned DNSes have less data consumption than the others. Known servers' DNSes were scored as '4'. For millions of users around the world are using known, safe DNS servers, such as Google DNS Server[7]. And unknown DNSes were scored as '1'. As mentioned in [15] there were number of perilous attacks made due to the vulnerabilities of DNS servers. Furthermore, if something is nondescript, no one may allege that it is reliable.

In this way user score consisted of four different components; usage score, operating system score, web browser score and DNS score. Coefficients of these components were different from each other. However, all of these components had a contribution to the final score. Components had a higher impact on the final score with respect to their influence on the network.

[6]https://nvd.nist.gov/

[7]https://developers.google.com/speed/public-dns/

B. Network Component Analysis

In this part, network and network components were examined independently from users. In other words, networks' scores depended on their network security parameters like Firewall, IDS. Many of these technologies sustain security of the networks, so enterprises ought to get service for security equipments from known network security companies if they claim to have a reliable network. In NESRAS, impression of the user score was higher than the system analysis score on overall score of the system. Because usage of the system, which is an answer of following questions; which web sites were visited by users, what kind of contents were downloaded by users and which email servers were chosen by users, shows the real impact on the network.

Initial score of the network components scoring step was '0'. The score rised in accordance with the predetermined components. If network involved these predetermined components, different scores of the each involved component were added to the total network components score. Some predetermined parameters and respectively their scores were given at Table 4. If the network had all these predetermined components, it got the highest score '5'.

TABLE IV: 6 DETERMINED NETWORK COMPONENTS

Network Components	Scores
Firewall	2
Anti-Malware Tools	0.5
Virtual Private Network (VPN)	1
URL Filtering	0.5
Anti-Spam Software	0.5
Intrusion Detection Systems(IDS)	0.5

Investigating vulnerabilities of the network components is another attractive topic for the network security. For this reason, scoring the network security vendors and their products are planned for the future work. Thus, system will offer the best option of components and vendors to make network as possible as secure.

IV. Results

The last part of the study demonstrated the results which were obtained by implementing NESRAS. Moreover some statistics about users in the network were presented. The network security simulator program was developed to test the NESRAS. The program took the input file as 'Comma-separated values' (CSV) file format to produce network user scores, and components of the examined network might be selected from predefined network products by way of the program. It produced a report about the users in CSV file format which included usage, operating system, web browser and DNS scores of the users. The program also produced bar charts to show statistics of the users. Charts were saved as image files to simplify the system utilization.

If a user in the network took a point more or equal to '3', NESRAS assigned the user as 'Standard User'. Standard users only affects the overall system score, but main purpose is to find 'Critical Users' who have taken a score less then 3 from the system. Critical users swing the balance of the system score. Network Score decreases as much as the number of critical users. 2697 different users were examined. System

assigned 2111 (almost 78%) users as Critical Users. Overall score of the users was found '2.807661'. It means, users were not a threat for network, but some users had hazardous usage. Thus experts ought to take security precautions of the network. Final score of the system was determined with adding overall user score and network components score. For instance, if network has all components listed at Table 4 except IDS, network components score becomes 4.5. Thus, total score is 3.707661 which refer to the stable network.

TABLE V: 10 USERS WHO HAVE LOWEST TOTAL USER SCORE

User Local IP	User Analysis Results				Total User Score
	Usage Score	OS Score	Web Browser Score	DNS Score	
193.255.165.131	1	4.3	3.5	1	2.175
193.255.169.103	1	4	3.5	4	2.375
193.255.163.154	1	4.3	3.5	4.5	2.46
193.255.160.251	2	4	3	1	2.5
193.255.161.127	1.5	4	3	4.5	2.541
193.255.165.251	2.32	3.3	3	1	2.543
193.255.161.190	2.33	3.3	3	1	2.55
193.255.168.244	2.4	3.3	3	1	2.583
193.255.161.221	1.57	4.3	3	4	2.589
193.255.170.153	2.44	3.3	3	1	2.6

Table 5 presents ten users who took the lowest total score from the system, and other scores of these users. User who has taken the lowest score '2.175' may become a threat for the network. Especially users whose usage scores are '1' may referred as critical users of the network. Because having usage score 1 means users visited solely hazardous web sites. Lastly, Categories of 'Unknown and Pornography' were the most visited web site categories by the lowest 10 users in the network.

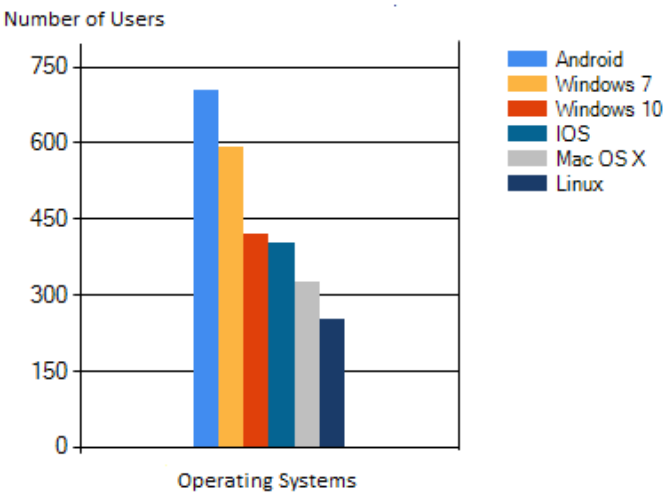

Fig. 1: Distribution of the most used 6 Operating Systems over the users

Figure 1-3 present the number of users and distribution of operating systems, DNSes and web browsers over the users via bar charts. According to these charts, the most used operating system as Android, the most preferred web browser as Internet Explorer and the most chosen DNS as Service Provider DNS were found in the devices which were used while connecting

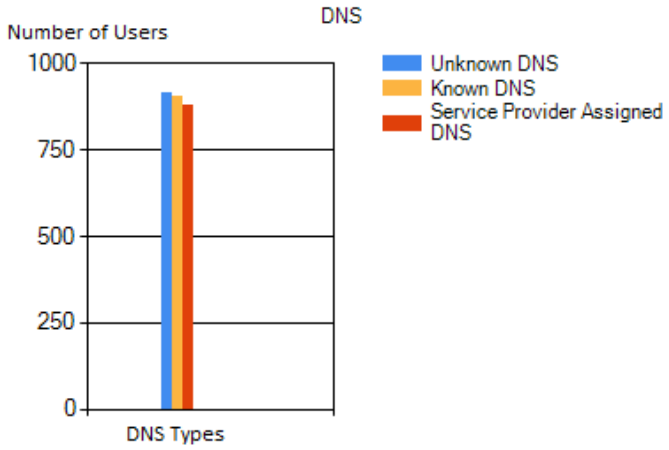

Fig. 2: Distribution of DNS platforms over the users

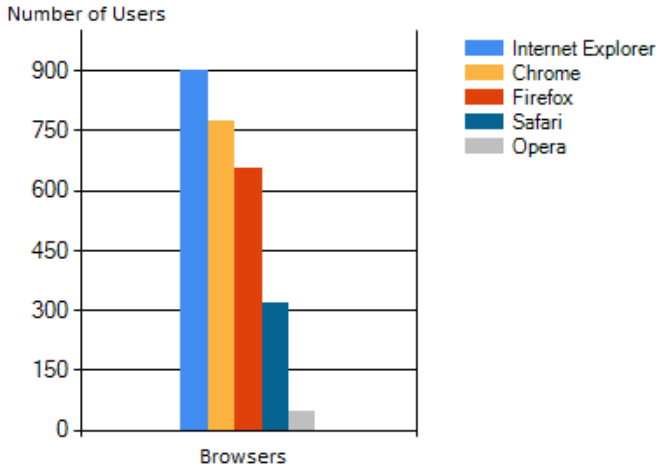

Fig. 3: Distribution of the most used 5 web browsers over the users

to the Internet in the studied network. Usage rates in charts may help to experts of the network while they take precautions for the network.

V. Conclusion

In this study, network users and network components are examined. A system was offered to score networks and users of the networks, and a network simulator program was created to test the system. Users were scored based on their usage, operating system, browser, and DNS information in created synthetic dataset. Comparing with the determined components in the system, network components were scored accordingly. System assigned to the studied network one of the colors; red, orange, yellow or green according to the total score. Users who had 10 lowest total user scores were presented. These users assisted to hold a view on the hazardous users of the network. Finally, distributions of the operating systems, web browsers and DNSes over the users were presented with bar charts.

REFERENCES

[1] B. Daya, "Network Security : History , Importance , and Future," tech. rep., University of Florida Department of Electrical and Computer Engineering.

[2] Q. Gu and S. Marcos, "Denial of Service Attacks Department of Computer Science Texas State University – San Marcos School of Information Sciences and Technology Pennsylvania State University Denial of Service Attacks Outline," pp. 1–28, 2007.

[3] B. M. Bowen, R. Devarajan, and S. Stolfo, "Measuring the human factor of cyber security," *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*, pp. 230–235, 2011.

[4] H. Abie, "An Overview of Firewall Technologies," *Telektronikk*, pp. 1–9, 2000.

[5] N. Chakraborty, "International Journal of Computing and Business Research (IJCBR) INTRUSION DETECTION SYSTEM AND INTRUSION PREVENTION SYSTEM : A COMPARATIVE STUDY Nilotpal Chakraborty," *International Journal of Computing and Business Research*, vol. 4, no. 2, 2013.

[6] HKSAR, "VPN Security," Tech. Rep. February, The Government of the Hong Kong Special Administrative Region The, 2008.

[7] Symantec, "Internet Security Threat Report," *Internet Security Threat Report*, vol. 20, no. April, 2015.

[8] N. Goel, "Analyzing Users Behavior from Web Access Logs using Automated Log Analyzer Tool," *International Journal of Computer Applications*, vol. 62, no. 2, pp. 29–33, 2013.

[9] "eWebLog Analyzer," 2010.

[10] "SARG," 2010.

[11] "NetIQ Ssytem Management," 2010.

[12] K. Oztoprak, "Profiling subscribers according to their internet usage characteristics and behaviors," *Proceedings - 2015 IEEE International Conference on Big Data, IEEE Big Data 2015*, pp. 1492–1499, 2015.

[13] "Market Share Statistics for Internet Technologies."

[14] "The Ultimate Security Vulnerability Datasource."

[15] M. Silic, J. Krolo, and G. Delac, "Security vulnerabilities in modern web browser architecture," *MIPRO 2010 Proceedings of the 33rd International Convention*, pp. 1240–1245, 2010.