Ramaiah Institute of Technology

(An Autonomous Institute, Affiliated to VTU)

MSR Nagar, MSRIT post, Bangalore-54

Computer Network Security (CS71)

Assignment

on

Network Security Scoring

Submitted by

Name of the students :	USN :
RAVIKUMAR	**1MS16CS076**
PRATHEEK S	**1MS16CS067**
RAJATH	**1MS16CS050**

In Partial fulfillment

of

4th year BE (CSE) Program

Department of Computer Science & Engineering

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

M.S.RAMAIAH INSTITUTE OF TECHNOLOGY
(Autonomous Institute, Affiliated to VTU)
BANGALORE-560054
www.msrit.edu, **2019**

Network Security Scoring

1. 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. Now a days protecting real time data is also a major challenge in the digital system. Data prevention and service providing to the client in the required manner is also great challenge because data encryption and delivery the required thing to the client include this; analyze the server and check the status of the server whether that hacked by someone or not.
Lot of people kept their data on the enterprise server and they more safety;

2. Keywords:

Network security; security scoring; Network user analyzing; Network component analyzing; Operating System

3. Explanation of the Paper Implemented

Universities, public and private enterprises and their networks security have critical importance on national security. 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. 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.

Next explained the basic concepts about the network security and real time data protection and malicious software or piece of programs that cause the system hack; internet is the major and very vast platform to share and communicate with each other this include the computer network and security also. Third party may steal the confidential information and make misuse; developed cyber attack includes the various things that could harm the client computer those are Viruses, Worms, Trojans, Bots, IP Spoofing, DoS Attacks others .

These are the hazardous and danger programs that destroy the client. Means that the targeted network will go down and huge loss will occur to that particular company or network. It also include the steal of confidential data. To prevent this kind of things, every enterprise network have the anti virus, anti-malware, firewalls, DNS, proxy server, VPN etc.. these acts as bridge between the sender and the receiver and mainly filter the required things and reduce the unwanted traffic so that security enhance and vulnerability will low; in this paper analysis work done more! Analyzing the user network and get the required data make the analysis and prediction that detects hazardous attacks finding the solution. Mainly we are concentrating more on the analysis of the enterprise network by using the log file of the user; finally in this approach making a model that could predict the network get hacked or not by analysis of the entire user activities as well as network security components;

For this work, they have suggested to use the log data files; such as Google analytics, AWStats and web log Expert; for cleaning the data we have to use the eWebLog, NetIQ, etc; , 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. This include the various task that cleaning and handling all the data from the log file. Make suitable for the handling all the variable which are required to analysis; this whole analysis include the building model for the future prediction;

3.1) 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 analytics, which was the first step of the system, was based on scoring the users in studied network. Dataset, which was used by author , 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 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). 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.

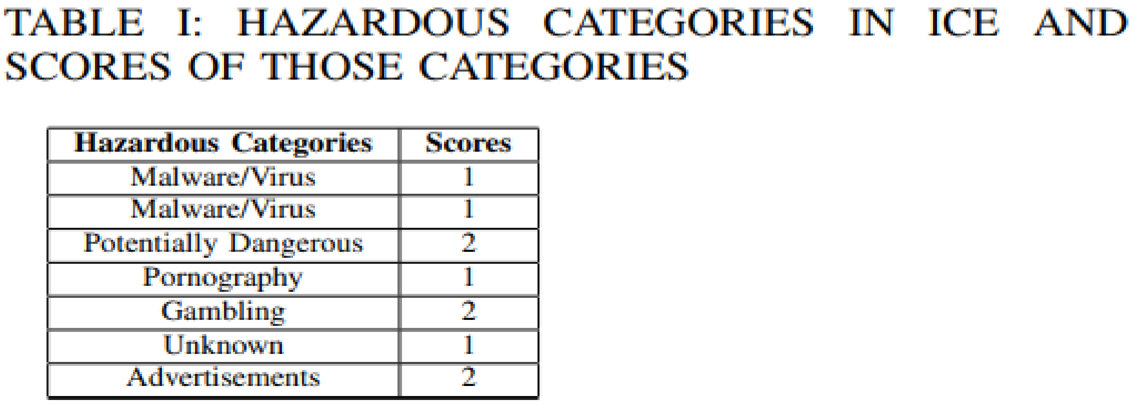


TABLE I: HAZARDOUS CATEGORIES IN ICE AND SCORES OF THOSE CATEGORIES

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

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. regarding vulnerabilities in National Vulnerability Database (NVD)

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 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

Web Browser	Score
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

B. Network Component Analysis:

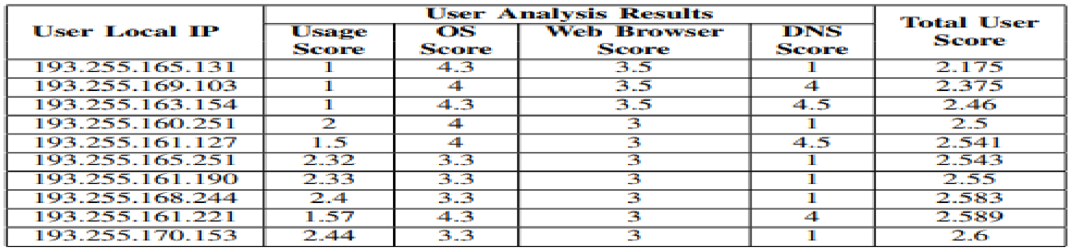
In this part, network and network components were examined independently from users. In other words, networks' scores depended on their network security parameters like Firewall, IDS. Many of these technologies sustain security of the networks, so enterprises ought to get service for security equipments 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.

Network components	**Score**

Firewall	**2**
Anti-Malware Tools	**0.5**
Virtual private Network (VPN)	**1**
URL Filtering	**0.5**
Anti-Spam Software	**0.5**
Intrusion Detection System (IDS)	**0.5**

RESULTS and Snapshots:

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

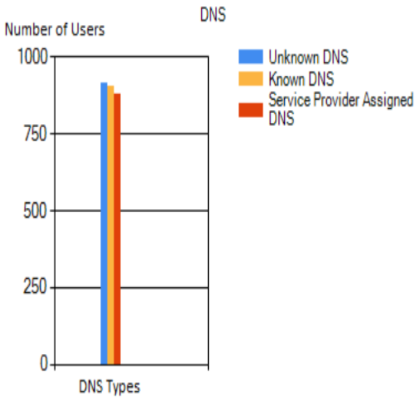


Fig. 2: Distribution of DNS platforms over the users

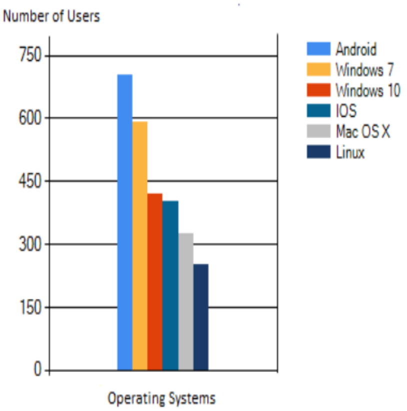


Fig. 1: Distribution of the most used 6 Operating Systems over the users

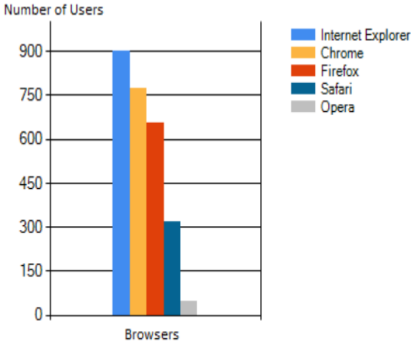
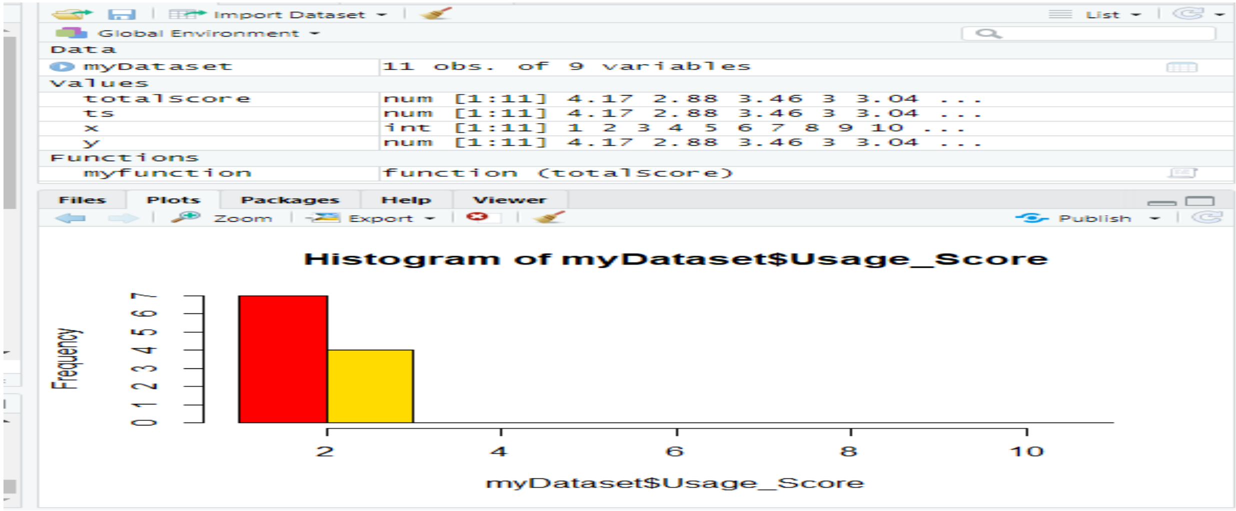


Fig. 3: Distribution of the most used 5 web browsers over the users

Final result and prediction range:



```
Data
  myDataset          11 obs. of 9 variables
Values
  totalScore         num [1:11] 4.17 2.88 3.46 3 3.04 ...
  ts                 num [1:11] 4.17 2.88 3.46 3 3.04 ...
  x                  int [1:11] 1 2 3 4 5 6 7 8 9 10 ...
  y                  num [1:11] 4.17 2.88 3.46 3 3.04 ...
Functions
  myfunction         function (totalScore)
```

Sudo code:

```
myDataset<-read.csv("paperDataset1.csv",header = TRUE)
#randDataset<-read.csv('paperDataset.csv',header = TRUE)

ts<-myDataset$Total_User_Score+myDataset$Network_socre
#ts<-randDataset$net_value
y<-ts
x<-myDataset$ip_values
totalScore<-ts

myfunction<-function(totalScore){
for(i in totalScore){

 if(i<1.5){
   plot(x,y,xlab="ip values",ylab="net values", col = ifelse(i < 1.5,'red','white'), pch = 19,main = "network might be in a
danger of attack" )

 }
  if(i>=1.5 && i<3.0){
    plot(x,y,xlab="ip values",ylab="net values", col = ifelse(i >= 1.5 && i<3.0 ,'orange','white'), pch = 19,  main = "some
problems in network")

  }

  if(i>=3.0 && i<4.0){
    plot(x,y,xlab="ip values",ylab="net values", col = ifelse(i >= 3.0 && i<4.0 ,'yellow','white'), pch = 19,main = "Stable
network" )

  }
  if(i>=4 && i<=5){
    plot(y,x,ylab="ip values",xlab="net values", col = ifelse(i >= 4 && i<=5.0 ,'green','black'), pch = c(19,8),main = " ideal
network" )

  }

}
}
myfunction(totalScore)
str(myDataset)
summary(myDataset)
hist(myDataset$Web_Browser_Score,myDataset$ip_values,col = rainbow(7))
hist(myDataset$DNS_Score,myDataset$ip_values,col = rainbow(7))
hist(myDataset$OS_Score,myDataset$ip_values,col = rainbow(7))
hist(myDataset$Usage_Score,myDataset$ip_values,col = rainbow(7))
```

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] 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

[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.

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

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