

BRO IDS Log files analyzer and visualizer

(Bachelor in Computer Science graduation project)

Ahmad Da'na -20121024

Mosa'ab AbuShanab -2012

Supervisor : Dr.Ali Hadi

Introduction

BRO is an open-source software, designed by Berkeley university for network traffic analysis and intrusion detection ,and is used for network forensics purpose, and is a fully passive network traffic analysis tool.

The software generates log files that log network interactions, and splits the results based on their application layer protocol (HTTP,FTP,DNS SSL ,SMTP and others)[1], however the data provided by the IDS is hard to deal with, In example of capturing big amount of traffic packets .

We are building a software that reads BRO-generated log files, analyzes them and generates visualized graphs and statistics based on the data provided by the log files; to ease the process of studying and analyzing the traffic and security of networks .

Data gathering

|  |  |  |
| --- | --- | --- |
| Stakeholder No. | Name and description | Data gathering method |
| 1 | Dr. Ali Hadi – professor at PSUT | interview |
| 2 | BRO IDS users | Questionnaires and interviews |
| 3 | Information Security masters degree students at PSUT | Questionnaires and interviews |

Functional requirements

|  |  |  |  |
| --- | --- | --- | --- |
| Requirement | Name | Description | Note |
| 1 | Accuracy | The program should provide accurate analytical graphs and statistical data using the appropriate statistical methods | \_\_ |
| 2 | Files | The program should be able to deal with BRO files as individual or as a group since the program separates the log files according to traffic type.  The program as well should be able to detect corrupted or unsupported log files provided by user. | \_\_ |
| 3 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Non-functional requirements

|  |  |  |
| --- | --- | --- |
| Requirement | Name | Description |
| 1 | Usability | The program should provide easy interactive UI |
| 2 | Performance and responsiveness | The program should be fluid and efficient in terms of performance and memory |
|  |  |  |
|  |  |  |

Requirements Analysis

References

[1]: BRO documentation   
<https://www.bro.org/sphinx/intro/index.html>

[2]