- Project Title

Network traffic log analysis

- Student Name

Weilun Li

- Student ID

1892748

- Supervisor Name

Ian Batten

- Project Category/Topic:

Security

Project Aim:

- In no more than three sentences, describe what you wish to achieve.

Analyze the traffic log data of the website to find out the abnormal traffic. Detect and predict abnormal traffic.

- Significance: Why is the project important?

Find abnormal traffic on the website immediately , so that the website can be found to be traffic attacked. A response can be made to prevent more serious impacts caused by the undetected attacks on the website traffic.

- Relevance: Your project needs to have a computer security, what is it?

It may have traffic attacks or DOS attacks, we need attack detection and attack prediction.

Related work:

- List the most relevant work in the area (with the help of the supervisor).

Data collection   Data pre-processing   Data analysis   Data presentation

Project Objectives/Deliverables:

- 5-10 concrete and measurable project objectives.

Data collection   Data pre-processing   Data analysis   Data presentation

- For each objective, a one line description of how you measure successful delivery.

Data collection ： Need a collection of completed data sets containing a standard set of audit data.

Data preprocessing : Pre-processing the collected raw log data through the program, such as cleaning, formatting, filtering out dirty data, etc.

Data analysis : It is the core content of the project. Use based on behavior analysis to analyze the logs. current activity is compared to the past activity and find any new behavior[1]. Contrast and analyze 4 features include: 1) source IP address 2) destination IP address 3) destination port and 4) packet size[2].

Data presentation : The data obtained from the analysis is visualized and generally displayed on a chart.

- Explain why these objectives are sufficient to achieve your project aim.

Because after achieving these goals, we can get the results of the data analysis and compare with regular data then find out whether there is abnormal data. Achieve network intrusion detection in some way.

Threat Model

- Security projects usually operate in the context of a defined attacker or threat landscape. What is it?

Data may be analyzed by using unsafe software.

Sensitive content may be included in the data.

Methodology:

- Description of approach to solve the problem.

Try to work offline when doing data analysis.

Data pre-processing.

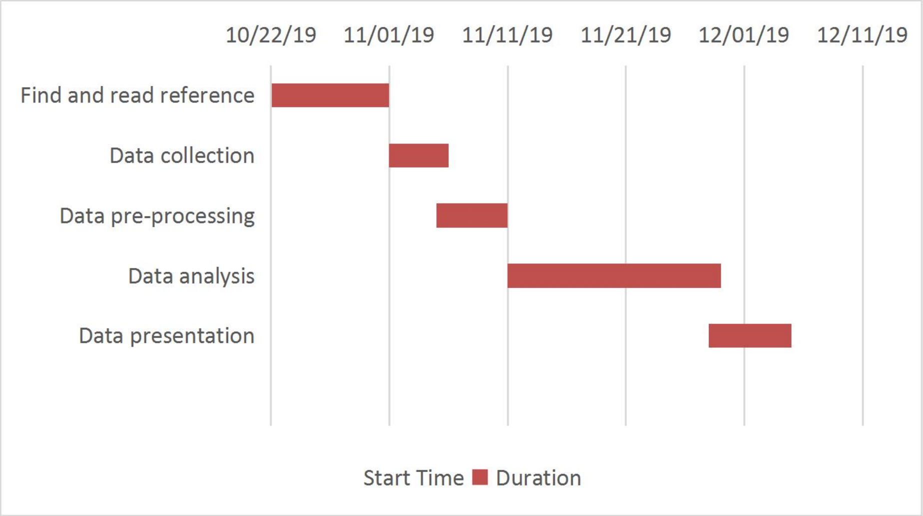
Project plan:

- Feasibility: Explain why your skills/expertise and the available resources are sufficient to complete the project in time.

Because the difficulty of the project is data collection and data analysis. The data collection step is first assisted by the supervisor, and the data analysis step can be done using the knowledge of the network security course and the security programming course.

- Gantt chart with tasks and milestones, reflecting the project objectives/deliverables.

Gantt chart (month/day/year)



- Explanation of Gantt chart

Find and read references 10 DAYS :

Find relevant literature and read it to learn how to analyze network traffic log.

Data collection 5 DAYS.

Data preprocessing 6 DAYS :

Pre-processing the collected raw log data through the program, such as cleaning, formatting, filtering out dirty data.

Data analysis 18 DAYS :

The core content of the project. Use based on behavior analysis to analyze the logs. current activity is compared to the past activity and find any new behavior[1]. Contrast and analyze 4 features include: 1) source IP address 2) destination IP address 3) destination port and 4) packet size[2].

Data presentation 7 DAYS :

The data obtained from the analysis is visualized and generally displayed on a chart.

Risks and contingency plan:

- What might happen that would prevent you from reaching the project objectives?

Too many data makes it difficult to complete all the data analysis. No typical results can be obtained, and the results are meaningless.

- What are the particularly difficult aspects of the project which you are worried about completing?

Data analysis model build failed.

- What is your contingency plan if there are problems?

Analyze as much data as possible after processing. Replace the data analysis model.

Reference

1. Sindhu Kakuru, “Behavior based network traffic analysis tool”, 2011 IEEE 3rd International Conference on Communication Software and Networks, 2011.
2. Nuttachot Promrit, Anirach Mingkhwan, “Traffic flow classification and visualization for network forensic analysis”, 2015 IEEE 29th International Conference on Advanced Networking and Applications, 2015.
3. Zhou Xiaopeng, “Traffic Analysis Technology Based on Network Security”, China Computer & Communication, vol.12, pp.201-202, 2019.
4. Hongyang Li, “Research and Realization of Detection of Abnormal Network Traffific Analysis”, Network security technology and application, vol.10, pp.63-64, 2013.
5. Fan Yu, “The analysis and design of an abnormal traffic inspection system”, University of Electronic Science and Technology of China, 2010.
6. Jing Qiu, “Research Progress of Network Traffic Forecasting Models”, Computer Engineering and Design, vol.33(3), pp.865-869, 2012.
7. Xiaodong Xu, Peng Bian, “Netflow-based abnormal traffic separation and classification”, Computer Engineering and Design, vol.30(21), pp. 4818-4820, 2009.

8. Cai Xue, “SNMP Protocol and Its Application in Network Management”, Ordnance Industry Automation, vol.22, pp.40-42, 2003.
9. Yang Zhijun, Tian Di, “Review of intrusion detection technology research”, Computer Engineering and Design, vol.27, pp.2119-2123, 2006.
10. Ji S Y, Choi S, Dong H J, “Designing a two-level monitoring method to detect network abnormal behaviors”, Information Reuse and Integration (IRI), 2014 IEEE 15th International Conference on IEEE, 2015.
11. Crovella M, Lakhina A, “Method and apparatus for whole-network anomaly diagnosis and method to detect and classify network anomalies using traffic feature distributions”, U.S. Patent 8, vol.869, 2014.
12. Promrit, Nuttachot, and Anirach Mingkhwan. "Traffic Flow Classification and Visualization for Network Forensic Analysis", 2015 IEEE 29th International Conference on Advanced Information Networking and Applications, 2015.