Vision and Scope Document

for

Network Threat Learning System

Prepared by:

Jan Michael Bernardo

Audrey Valencia

Adrian Balarbar

Ruy Josel Verano

Gavriel Mercado

1/17/17

Table of Contents

1. Business Requirements

The members of the group, along with their adviser came up with the requirements of the system that they are going to implement. These are the following things the system must be able to do:

- Detection of attacks and vulnerabilities
- Logs attacks that occur in the system
- Logs the frequency of attacks
- Allows identification with detailed information about attack

1.1. Background

The original members of the group are Digital Forensics Majors, so they thought it would be suitable to have a research that focuses on security, that will also help them to be more knowledgeable and develop their skills in the security field.
Asia Pacific College is a center for IT excellence so to further enhance the order of operations in the ITRO in terms of network security. The team will use Asia Pacific College (APC) as a piloting company to be able to test out the system.

1.2. Business Opportunity

The potential market of this innovation are those companies that have trouble securing their network and other valuable assets. Especially nowadays where in new exploits and networks are made almost everyday to gather sensitive information or destroy an infrastructure.

1.3. Business Objectives and Success Criteria

The objective of this innovation is to provide a system that will be able to efficiently identify zero-day attacks, learn about zero-day attacks, and analyze zero-day attacks. The success measures of the system are more gathered information and new generated rules.

1.4. Customer or Market Needs

Network administrators have a difficulty in securing their network in an environment where in newly made attacks are made everyday. The system will help network administrators lessen their workload. The system will also gather information from attacks, learn different patterns of attacks.

1.5. Business Risks

One of the risk that the developers are trying to manage is the lack of knowledge since the area of network security is very broad. The researchers require vast knowledge on network security. Another risk is that the time constraint of the team developers.

2. Vision of the Solution

The system will improve as more attacks and threats are logged and dealt with. This will allow the company to identify and handle the problem quicker and easier.

2.1. Vision Statement

The team intends to provide a system that will help companies improve their security by identifying and logging unpredictable attacks, thus minimizing potential problems and decrease recurring attacks.

Major Features

- Detect known attacks base from the signature base engine
- Record all attacks
- Categorize the known attacks
- Monitor the frequency of attacks
- Alert admin/s of attacks.
- Learning of zero day attacks.

2.2. Assumptions and Dependencies

Dependencies:
- Database to log attacks
- SNORT
- A Honeypot server

Assumptions:
- A basic knowledge of how to use SNORT
- A basic knowledge of setting up a honeypot server

3. Scope and Limitations

This project aims to help network administrators to efficiently secure their network. The project primarily focuses on detection of network attacks and correlation of attacks. The system can monitor any type of network attack, as long as it is in the parameter of the rules stored in the database.

3.1. Scope of Initial Release

1. The system will monitor any type of attack

2. The system will be able to learn attacks
3. The system practices the three types of correlation

3.2. Scope of Subsequent Releases

In subsequent release, the system will be able to learn attacks based on different patterns of attack.

4. Business Context

Since our team is making a system that is specialized in security, it could affect many companies. where in it includes:

- The security of the network will increase
- The security analyst doesn't need to monitor the network all the time because our system will alert whenever there are threat to the network.
- Reduce workload and errors.
- More accurate records.

4.1. Stakeholder Profiles

Stakeholder	***Major Value***	***Attitudes***	***Major Interests***	***Constraints***
User	*improves the system*	*Reports attacks occurred.*	*ease of use*	*Report only*
System Administrator	*Monitors logs; creates rules*	*Security expert; critical thinking*	*Determine and fixing errors and inconsistencies*	*no budget for retraining*
Security Analyst	*tunes attacks*	*decides fast; has more patience; learns fast*	*automatic error correction; easy to use*	*Limited access*

4.2. Project Priorities

Dimension	***Driver (state objective)***	***Constraint (state limits)***	***Degree of Freedom (state allowable range)***
Schedule	*release 1.0 should be available at the end of the course*	*Time Constraint*	*90 - 100% of the utility functions must be done*

Features	*The main functions must work properly*	*simple functions designs in release 1.0*	*70-80% of high priority features must be included in release 1.0*
Quality	*Provides new and reliable tool for security*	*expected error and bugs in release 1.0*	*90-95% of user acceptance tests must pass for release 1.0*
Staff	*knowledgeable in network security*	*maximum team size is 6 developers + 4 testers*	*90 - 100% of the time should be used for release 1.0*
Cost	*spend at least the minimum budget*		*budget overrun up to 15% acceptable without executive review*

4.3. Operating Environment

The system will be set up in the honeypot server. The users of the system will be the security administrators, security analyst, and the employees who use the computer. The system will function 24 hours to monitor the attacks happening in the network. The users will access the system when the system alerts the admin, when the admin checks and add rules, when the system analyst checks and tunes alerts, and when there are changes made.