System Specification

Author: CMU Team

Date: 09/23/2005

Table of Contents:

1. Introduction

Despite a multitude of efforts and a wide variety of approaches devoted towards computer security, guaranteeing secured computer networks is still a grave challenge. We propose a system that would contribute significantly towards these efforts.

The system would provide a dual functionality:

- Enhancement of vulnerability scanning tools reports
- Intelligent monitoring of traffic to detect possible attacks

1.1. Enhancement of vulnerability scanning tools reports:

The proposed system would enhance the power of vulnerability scanning tools such as Nessus by categorizing the different vulnerabilities as well as the possible security attacks that the host is likely to yield to due to these vulnerabilities. The different vulnerabilities identified by Nessus would be appropriately mapped into these vulnerability categories, and the corresponding security attack type would be identified, hence providing more useful and easy to understand information that would enhance the usability and effectiveness of Nessus. In addition, a user-friendly and visually interactive interface would be included that would enable users to better understand the reports generated by Nessus.

1.2. Intelligent monitoring of traffic to detect possible attacks:

The proposed system would also provide an added 'intelligent' component that would monitor the flow of traffic in the network, analyze it and detect possible attack scenarios. The module would possess the ability to behave as both – a misuse detection as well as anomaly detection system. Hence, it would be able to identify the type of attack, if the attack is of a known attack type and would also be able to identify an attack as 'anomalous' if the attack is new and previously unseen. This would be a significant leap from the functioning of standard vulnerability scanning tools such as Nessus.

The system architecture and the technical specifications of proposed system are provided below:

2. System Architecture

As shown in Fig.1, the procedure would include four phases: information collection, data analysis, report generation, and presentation. In the first phase, information collection, Nessus client programs would be installed and set up on the protected machines. Also traffic would be captured on router span port or PCAP on the firewall. The data analysis phase would include both vulnerability and traffic analysis. The vulnerability scanning function would come from Nessus with its own vulnerability knowledge base. Possible vulnerabilities would be evaluated according to the response from Nessus clients. Our system would provide the traffic analyzer, which would analyze the network traffic collected in the previous phase. In the third phase, report generation, both vulnerability and attack reports would be generated based on the analysis carried out in the previous phase. In the final phase, these reports would be presented in a web-

based utility with a user-friendly and visually interactive interface. Collectively, these four phases would offer an effective dual functionality of enhancing the effectiveness of Nessus and also providing an intelligent module that monitors the traffic to detect possible attacks.

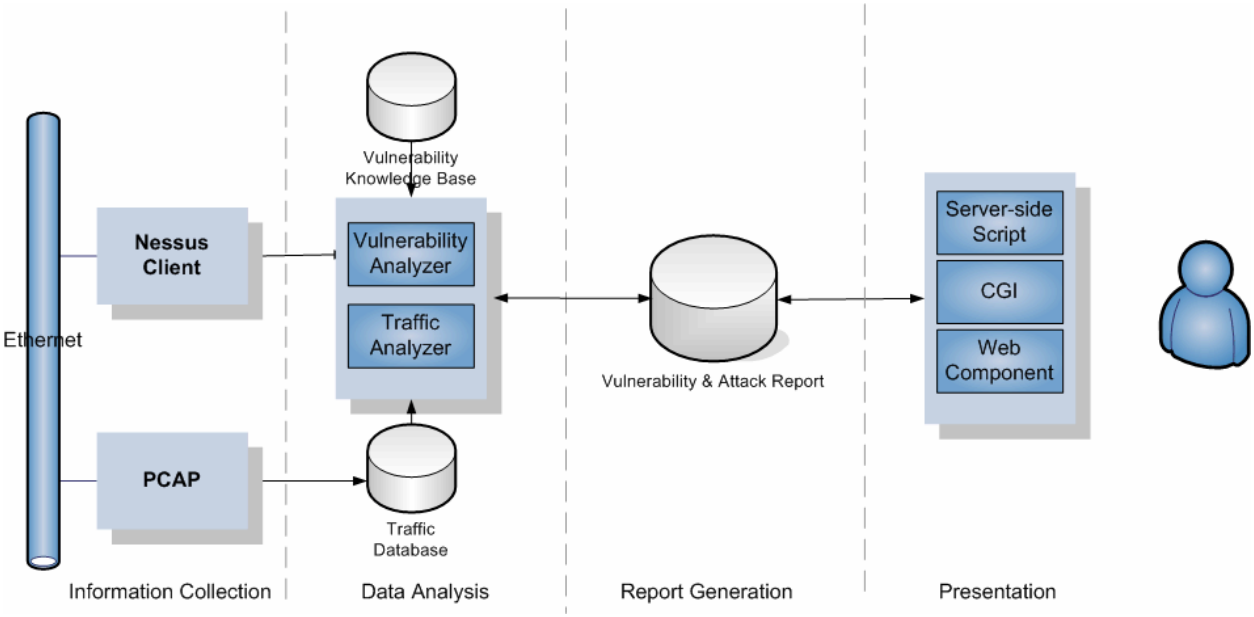

Fig. 1: System Architecture

3. Technical Specifications

3.1. Information Collection:

As shown in Fig. 2, Nessus clients would connect to the Nessus server via Ethernet. Internal firewalls drop the rapid-fire connections generated by vulnerability scanners, and are thus a problem that plague the vulnerability assessment teams. The Nessus serves would thus be put on the local loopback with Nessus clients. There are two approaches being considered to capture network traffic. One is to use the span port in the router. This approach has the advantage of not affecting the operation of local machines. However, all network administrators cannot access the router and not all routers support this function. The alternative approach is to deploy sensors on protected machines and report the network traffic regularly. This would however, increase the load on protected machines and in turn decrease the performance of the local network. Both approaches are currently being evaluated. All traffic information would be stored in a MySQL database.

3.2. Data Analysis:

Pattern recognition and machine learning techniques would be at the heart of this module. Pattern recognition techniques not only provide us with the tools to match attack signatures and hence identify the type of attack, but also provide us with the generalization power to identify a new type of attack as anomalous behavior and report it as a potential attack. Pattern recognition

techniques have been shown to provide a good compromise between the sensitivity of the intrusion detection system to identify attacks, and lowering the false alarm rates. Neural networks would be used as a classification tool to identify attack scenarios. Several different sources such as traffic statistics, contents information and basic information about the connections can provide useful indications regarding the possibility of an attack. Information would be combined from these different sources using sophisticated pattern recognition algorithms to make more reliable decisions about whether an observed traffic pattern is a potential attack or not.

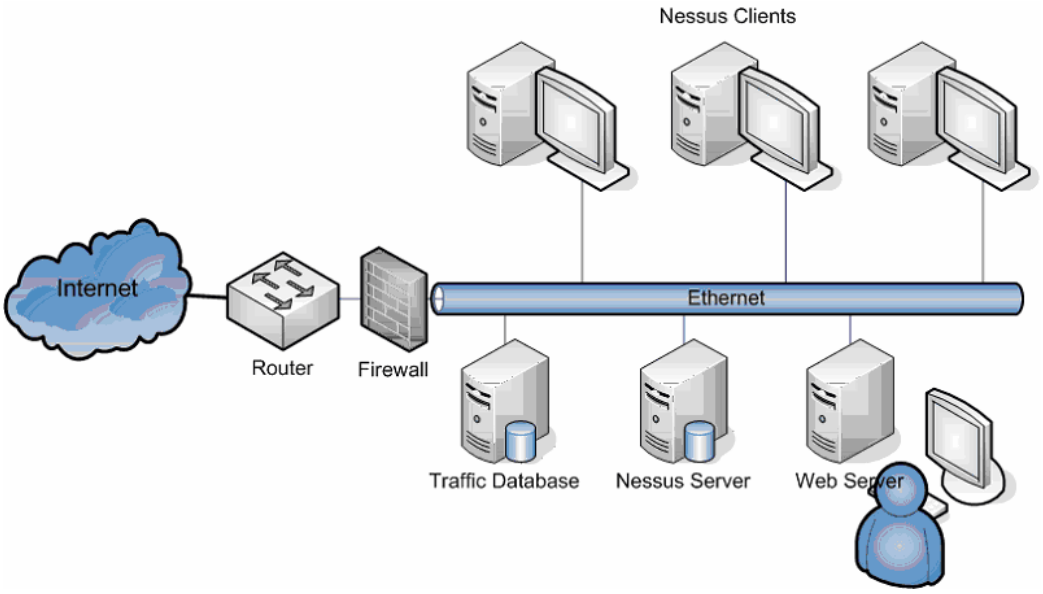

Fig. 2: Deployment Scenario

3.3. Report Generation and Presentation:

Apache would be used to build a web server which offers a web-based interface to evaluate all the reports generated by both the Nessus server and the traffic analyzer. Nessus provides several report files in different formats. Most of these different format styles seem lengthy and obscure for users. Thus we would provide a user friendly and easily accessible interface via a web based report presentation and report the appropriate mappings of the different vulnerabilities identified by Nessus into the different vulnerabilities and attack categories. The status of the network traffic as analyzed by the traffic analyzer (normal or malicious – and possibly the specific type of malicious activity) would also be shown through the same interface.

4. Summary

To summarize, the proposed system would not only provide an enhancement to vulnerability scanning tools such as Nessus in the form of a plug-in to make the reports more user-friendly, but more significantly, would provide an intelligent traffic analyzer module, that makes it a more complete and versatile computer security tool.