Open Source Security Appliance

by

Adam J. Plas

Submitted to
the Faculty of the Information Technology Program
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

University of Cincinnati
College of Applied Science

June, 2007

Open Source Security Appliance

by

Adam J. Plas

Submitted to
the Faculty of the Information Technology Program
in Partial Fulfillment of the Requirements
for
the Degree of Bachelor of Science
in Information Technology

Adam J. Plas	Date
Mark Stockman, Faculty Advisor	Date
Hazem Said, Ph.D. Department Head	Date

Acknowledgements

I would like to thank the faculty and staff at the University of Cincinnati's College of Applied Science for accepting and believing in my project. I would like to give special thanks for Aaron Rucker, system administrator at the University of Cincinnati's College of Design, Art, Architecture and Planning for giving me technical advice and hardware support. I would also like to thank all of the anonymous posters in the hundreds of forums I posted questions and found answers; truly there was no greater technical help to me than your help. Finally, I would like to give thanks and love to Amanda and Addison, my amazing wife and daughter, for helping me through this project and my senior year.

Table of Contents

Section **Page**

List of Figures

Figure Number **Page**

Abstract

The Open Source Security Appliance (OSSA) has been developed to provide small organizations with tools that can provide network usage, security and vulnerability assessments. Many organizations do not have the budget to put dedicated security appliances in place, nor the personnel to monitor the output. Open source software can help to monitor a network, but is often difficult to set up and the output can be difficult to read. The OSSA brings together widely used and well supported tools in an easy to configure and deploy appliance. The OSSA is based on Ubuntu Linux, with Snort, Nessus and NMap providing the monitoring solution. The web front-ends BASE and Inprotect are used to provide easy to understand outputs for a system administrator in a hurry. One of the main features of the OSSA is a web portal that provides connections to the web front-ends as well as network diagrams, product documentation and scenario response information. The OSSA has been rolled into a Linux distribution that can be installed as a standalone appliance or as a virtual machine.

Open Source Security Appliance

1. Statement of the Problem

As organizations are becoming more interconnected and dependent on outside resources, it has become clear the information security must be considered in the operation of any sized network. Large businesses and enterprises can afford to hire dedicated personnel to monitor specialized equipment for possible attacks. Small and medium-sized businesses that can not afford a dedicated security infrastructure often use a collection of tools that do not necessarily give a complete picture of network security and may store the results of the tools in different locations, which can make analysis impossible. There are few dedicated security appliances marketed towards small and medium-sized businesses, and those that are offered allow the system administrator only limited control over what can be changed. Small and medium-sized businesses with limited budgets and personnel need to have tools that are easy to implement and configure with easy to read outputs to monitor network security.

2. Description of the Solution

In order to provide a easy to implement and robust infrastructure to small and medium-sized businesses, an Open Source Security Appliance (OSSA) was developed for use within a network. As the name suggests, this appliance uses a wide variety of open source technologies to monitor and secure the network. In conversations with Aaron Rucker, the system administrator at the University of Cincinnati's college of DAAP (1) and Randy Diekmeyer of PEDCo E&A (2), it became apparent that implementing open source security tools was commonplace on host computers, but much

more complicated in a network environment. The open source tools that are available are very powerful and useful, but require time and patience that a harried system administrator may not have. After discussions with Rucker and Diekmeyer, the idea for an ideal "soft" appliance appeared. This soft appliance included these features:

- Popular and widely used open source applications that are regularly updated;
- Built on a stable and supported Linux distribution;
- Allow for expansion of an organization;
- Collect all the monitoring information in a centralized location using a client-server relationship;
- Provide single seat administration through a web interface;
- Easy integration into a network as a VMWare appliance;

My solution has two components at its core: sensors and a correlation engine. The sensors have two powerful open source security tools installed to scan a specific network segment for intruders and potential vulnerabilities. Snort is an intrusion detection system, or IDS often called the "de facto standard in intrusion detection" (3). Nessus is a vulnerability scanner, a three-time first place winner in a survey conducted by SecTools.org (4). These tools allow a system administrator to see attacks that are occurring so they can be stopped, as well as alerting about vulnerabilities that could allow attacks to succeed.

Each sensor scans a particular network segment, and than sends the results to a centralized correlation server. The server runs the web-based front ends for Snort and Nessus, called BASE and Inprotect. Both web-based front ends provide analysis through graphical outputs and centralized administration through a web browser.

System administrator needed a single point of contact for both of the web-based front ends, so a management portal is included in my project. This management portal is a collection of data and documentation that would be useful to a system administrator during an attack or network outage. The documentation included with the default installation will detail disaster recovery documentation and outline procedures that a system administrator can create to streamline recovery during an attack. Network information such as diagrams and schematics also have a place within the portal so that pulling up physical circuits is not a problem during an emergency. This documentation will also be useful for other IT workers in the organization, especially co-op students who often do not have the time to learn all of the procedures and may not remember what to do in an emergency. This management portal is written in HTML to make it very easy for a system administrator with limited background in web development to upload documentation and make changes.

By utilizing a client-server (or sensor-correlation engine) relationship, a system administrator is free to deploy a solution that suits the needs of the organization instead of being forced into an awkward situation with a locked down appliance. Each sensor can be configured to meet the needs of a particular network segment. For example, if an organization is running a Demilitarized Zone (DMZ) outside the network for web and mail servers, it would be helpful to watch for attacks on port 80 for web attacks and port 25 for SMTP attacks, but not necessarily helpful to look for those same attacks on the file server network that is only reachable from inside the network.

The sensors and correlation engine are delivered as VMware machines, ready for installation into VMWare Server. This is an important part of my solution, because it

allows the sensors and correlation engine to be run on currently existing and deployed hardware. VMWare server is freely available for installation on all major platforms and can be used to host OSSA as well as other virtual machines and appliances the system administrator may want to use. The only hardware costs associated with this project are possibly adding multiple network cards to the machines that will be hosting either the sensors or the correlation engine.

A recent survey by the Internet Storm Center asked "What is Your Security Budget?" 59.1% of the respondents stated that "Our coffee budget far exceeds our security budget." (5)