OD/ITAO
NIHRFC0048
Category: Standards

Helen Schmitz / Joe Klosky
OD
January 2010

Intrusion Detection Systems (IDS) Brick
V1.0

Status of this Memo

This document proposes an update of a technical standard for the National Institutes of Health (NIH) and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Table of Contents

OD/ITAO
NIHRFC0048
Category: Standards

Helen Schmitz / Joe Klosky
OD
January 2010

1 Introduction

This document updates the NIH Technical Architecture Standard for Intrusion Detection for the NIH community.

2 Description

Intrusion Detection is the practice of monitoring network traffic electronically and creating triggers for events of questionable value to the organization. These events will include, but are not limited to: access attempts, network worms, network bots, SPAM, unauthorized file copies, and other events potentially known as high risk.

Intrusion Detection can be broken down into two parts: system monitoring / logging and the deeper analysis of the logs for risk events.

System Monitoring and Logging. Identifying and reacting to security incidents in real-time requires comprehensive system and network monitoring. Intrusion Detection Systems are either software or hardware appliances that have internal capabilities and features to perform alerting of events based on preselected or custom triggers. Based on the alerts, security analysts can analyze live events, and depending on the solution, some limited historical logging as part of the feature set of Intrusion Detection Systems. Most Intrusion Detection Systems, due to limited features and logging retention space, export logs to other systems or storage for deeper analysis. Also, if aggregate alarms and other information from disparate IDS systems is needed to correlate events and identify trends, then tools outside of this brick may be needed.

Vulnerability Analysis. Internet-based attack tools are becoming increasingly sophisticated and, at the same time, increasingly easy-to-use. NIH's network could contain vulnerabilities that attackers can exploit to gain access, even when NIH has secured the network perimeter with firewalls and intrusion detection systems. In order to proactively find and plug such holes, NIH will require the use of both vulnerability assessment products and vulnerability assessment services. Some capabilities and functions existing inside of IDS tools require larger storage and better tools for deep analysis. Please refer to NIHRFC0049 for additional Vulnerability Analysis tools.

3 Intrusion Detection

This brick provides baseline information and the future direction for deploying Intrusion Detection inside the system boundary of NIHnet.

Helen Schmitz / Joe Klosky
OD

Table 1. Intrusion Detection Brick

Baseline Environment (Today)	Tactical Deployment (0-2 years)	Strategic Deployment (2-5 years)
■ IBM Proventia (ISS) ■ Snort (Open Source)	■ IBM Proventia (ISS) ■ Snort (Open Source)	■ IPS products ■ TBD
Retirement Targets (Technology to eliminate)	**Containment (No new deployments)**	**Emerging (Technology to track)**
■ None	■ ISS RealSecure	■ Multi-function network appliances ■ Unified Threat Management (UTM) products

Comments

- Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs for new products.
- Some baseline products have been designated as Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as low as the selected Tactical and Strategic products.
- NIH participates in the DHS Einstein situational awareness practice and benefits from cyber reports from DHS US-CERT derived from Einstein.

4 Contact

To contact the NIHRFC Editor, send an email message to EnterpriseArchitecture@mail.nih.gov.

5 Changes

Version	Date	Change	Authority	Author of Change
0.1	12/06/09	Initiation		Joe Klosky
0.2	01/20/10	Minor formatting changes	NIHRFC0001	Kiley Ohlson
0.3	03/14/10	Integrated Comments and Responses	NIHRFC0001	Kiley Ohlson
0.4	03/22/10	Integrated changes requested by ITMC EA Subcommittee	NIHRFC0001	Joe Klosky
1.0	04/27/10	Approved by the ARB	ARB	Kiley Ohlson

6 Author's Address

Helen Schmitz / Joe Klosky
OD/Office of the Chief IT Architect, NIH
10401 Fernwood Road, Room 3NW10B
Bethesda, Maryland 20817-4800
Phone: 301-496-2328
Email: schmitzh@mail.nih.gov
Email: joe.klosky@nih.gov

7 Summary of Comments

Comment:

I thought that this brick was not broken out well for its implementation. It identifies ID into two parts: logging and analysis. But, then it adds vulnerability analysis covered in another brick sort of randomly. Vulnerability analysis is not intrusion detection. One looks for vulnerabilities to threats. The other looks for active intrusions. The tactical deployment tools mention only a whole different category of real time network traffic analysis. For me, intrusion detection can be accomplished in real time at the network with analysis tools. They can either sample traffic to the side or analysis in real time in line with the traffic. The other side of intrusion detection can be done through logs. Log consolidation is a good thing but not easily managed or all inclusive. Defense in depth will be crucial to log gathering and IDS within the logs, esp. in near real time, as rules are created for log analysis. I think it will be important to use only one or two tools for log consolidation because good IDS work needs rule creation within the tools. Rule creation is not easy. I think that the brick should group into real time network IDS/IPS tools and Log consolidation IDS work (not real time, but host based logs make this needed). Also, IDS log analysis of the firewall logs is a tremendous benefit but challenging for the firewalls to do on their own. This single firewall log IDS work could be a third tool because its rule set will be unique and the volume extreme. Our internal creation and sharing the IDS rules created will be crucial to the success of any log consolidator IDS capability.

Response:

Yes, this is a good point. We refreshed the current brick with known technology versions within NIH. We invite additional feedback to other technologies currently in use at NIH but unknown to the rest of the IT community. We agree with your thinking in that IDS alerts have potential for false positives. We believe for an environment with multiple sources of alerting and logging, that tools outside the IDS are better suited for deep analysis and correlation. We invite participation in deeper looks into this technology as part of the ISSO groups coordinated by Dan Sands the NIH CISO or as domain teams instantiated and authorized by OCIO.

Comment:

We agree with comment that vulnerability analysis appears to be disjointed in this brick, however, we believe vulnerability analysis does belong in this brick, but with a different emphasis. NIH should tactically deploy IDS/IPS tools that have vulnerability analysis tools integrated within them for correlation and quicker incident response and remediation. An important aspect of the evaluation of the degree of risk involved with an intrusion, or possible intrusion, is whether the system is actually vulnerable to the exploit that is being attempted. We should choose tools that provide vulnerability details of a system at the same time real-time

alerts about a malicious behavior types that can exploit that behavior are happening. The administrator can then work with system owners to make a risk based decision about the recommended remediation.

Response:

We agree that the industry trend seems to be towards more IPS solutions (detect and block). We also hear the industry struggle with the “baked in” capabilities of IPS tools and appliances alone. We will continue to monitor the Security Engineering work at NIH and report standards as they become well known or if prudent, publish them publicly.