

# Vulnerability Management Tools Brick V1.0

## Status of this Memo

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

## Table of Contents

1	Introduction.....	2
2	Description.....	2
3	Contact .....	3
4	Changes.....	4
5	Author's Address .....	4
6	Summary of Comments .....	5

## 1 Introduction

This document updates the NIH Technical Architecture Standard for Vulnerability Tools for the NIH community.

## 2 Description

Vulnerability Tools cover a wide range of IT security functionality from general network vulnerability scanners to application exploitation detection.

Internet-based attacks are becoming increasingly more sophisticated. NIH's network could contain vulnerabilities that attackers may exploit to gain access, even when NIH has secured the network perimeter with firewalls, intrusion detection / prevention systems. This is especially true for web based applications available for use outside of NIH. In order to proactively detect, classify, and remediate. NIH will require the use of vulnerability assessment tools / products and vulnerability assessment services to properly assess emerging threats and to the NIH infrastructure.

This brick provides baseline information and the future direction for vulnerability tools at NIH.

**Table 1. Vulnerability Tools**

Baseline Environment (Today)	Tactical Deployment (0-2 years)	Strategic Deployment (2-5 years)
<ul style="list-style-type: none"> <li>■ Citadel Hercules</li> <li>■ eEye Retina</li> <li>■ IBM AppScan</li> <li>■ ISS Internet scanner</li> <li>■ Nessus</li> <li>■ NMAP (Open Source)</li> <li>■ LANGuard</li> <li>■ Metasploit (Open Source)</li> <li>■ MS Baseline Security Analyzer</li> </ul>	<ul style="list-style-type: none"> <li>■ Network               <ul style="list-style-type: none"> <li>■ eEye Retina</li> <li>■ Metasploit (Open Source)</li> <li>■ NMAP (Open Source)</li> <li>■ Sara Scan</li> <li>■ Tenable Nessus</li> </ul> </li> <li>■ Applications               <ul style="list-style-type: none"> <li>■ IBM AppScan</li> <li>■ Metasploit</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>■ Network               <ul style="list-style-type: none"> <li>■ TBD</li> </ul> </li> <li>■ Wireless Network               <ul style="list-style-type: none"> <li>■ TBD</li> </ul> </li> <li>■ Applications and Software               <ul style="list-style-type: none"> <li>■ TBD</li> </ul> </li> <li>■ Multi-Purpose               <ul style="list-style-type: none"> <li>■ TBD</li> </ul> </li> </ul>
Retirement Targets (Technology to eliminate)	Containment (No new deployments)	Emerging (Technology to track)
<ul style="list-style-type: none"> <li>■ None</li> </ul>	<ul style="list-style-type: none"> <li>■ ISS Internet Scanner</li> <li>■ LANGuard</li> <li>■ MS Baseline Security Analyzer</li> <li>■ Citadel Hercules</li> </ul>	<ul style="list-style-type: none"> <li>■ TBD</li> </ul>
Comments		
<ul style="list-style-type: none"> <li>■ 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.</li> <li>■ 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.</li> <li>■ NIH did not specify any one preferred Wireless Network scanner at this time. Many exist in this area of network tools. More work is required to narrow the many choices for Wireless network scanners for NIH network administrators and security analysts.</li> <li>■ Watchfire acquires Appscan and IBM acquires Watchfire in 2007</li> <li>■ Nessus is acquired by Tenable Security</li> </ul>		

### 3 Contact

## 4 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	03/14/10	Integrated changes requested by ITMC EA Subcommittee	NIHRFC0001	Joe Klosky
1.0	04/27/10	ARB Approved the NIHRFC	ARB	Kiley Ohlson

## 5 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](mailto:schmitzh@mail.nih.gov)  
Email: [joe.klosky@nih.gov](mailto:joe.klosky@nih.gov)

## 6 Summary of Comments

### **Comment:**

I am not sure that the break-out for this technology area is the best option. The document reduces the Vulnerabilities Tools into network, applications, and, someday, software code tools. However, there are other ways to break down the market space. Most of the time scanners for vulnerabilities are either network base or host based. They either have no OS or application privileges when they scan (network based) or they assume privileges of the host to scan (host based say using the AD permissions). A primary need for vulnerability scanning we have not mentioned is scan on attachment to the network for VPN or new systems that come on line. The brick doesn't mention any integration with network asset management tools which would detect what to scan. it doesn't mention the HHS tools in place such as Gideon SecureFusion (Symantec CCS or ESM again due to acquisition). it doesn't mention allowance for defense in depth tool in place at some ICs (e.g. EIQ). Consistency is a problem since the tactical breakout has network and applications but not operating systems. I think it sort of mixes the operating base of the scanner with what it being scanned. We can either go with tools identified by what they scan or how they are installed and privileged. In general scanners are either non-privileged or network based and focused on applications or O/S issues; or privileged and focused on OS, application issues, network issues, on-connect scans, etc. I think the document could be more robust in defining its market space. In general brand consolidation and product suites will continue to weaken the market space by forcing us to by into one solution and its weakness and support issues without any cross coverage and confirmation of findings. We need to be careful to allow defense in depth verification because as these products get consolidated into suites there complexity forces them to fall off quality quickly.

### **Response:**

We agree that scanners tend to fall into the two main categories of network base or host based. Security penetration experts will also perform tests from inside and outside user or location perspectives. This standard is not designed to dictate one tool unless there is clear consensus from the NIH technical community. We invite participation in workgroups to dig deeper into this space. We agree comparing existed well known NIH tools to new and emerging tools to see if domain teams are warranted to expand the NIH standards.