@JASON M OLIVER

Proper Depth & Breadth for Vulnerability Analysis and Fun with Tailored Risk Reporting Metrics.

DEPTH TESTING

- No Authentication vs. Authentication
- Requirement; FIPS 199 High Systems / NIST SP 800-53a Rev 3
- Validation - CoverageValidate.java
  - Nessus PluginID: 21745 - Failed to Authenticate
  - False Negative Bug; if you have a local firewall that blocks auth ports but not OS identification, it will not fire.

BREADTH TESTING

- Inventory to System Boundary Coverage Analysis
  - Know whats on & should be on your network!
- Requirement; NIST SP 800-53a Rev 3 (Inventory & Network Auth)
- Validation - CoverageValidate.java
  - Missed Hosts
  - Extra Hosts

PTES

- Q: What is this "Penetration Testing Execution Standard"?
- A: It is a new standard designed to provide both businesses and security service providers with a common language and scope for performing penetration testing (i.e. Security evaluations).
- http://www.pentest-standard.org/index.php/Vulnerability_Analysis

THE QUESTIONS

- What is the X worst machine(s)?
- What is the over all risk level of my network?
- What fix would have the most risk reduction effect?

WHAT IS A MEASUREMENT?

- Measurement: A quantitatively expressed reduction of uncertainty based on one or more observations.

How to Measure Anything: Finding the Value of Intangibles in Business - By Douglas W. Hubbard

A MATH SOURCE

- Why & What source to leverage for math?
  - Is the impact more important that the threat criticality, by how much; 1x, 10x, 100x?
- NIST Risk Assessment Framework = Less Debate
  - 1 x 10 ratio of Threat to Impact

IMPLEMENTATION CODE

- XMLVulnStats.java - Works with Nessus V2 Files
  - Available @ www.blackhat.org today.
- Command-Line: java XMLStatsVuln output.xls *.nessus
- Features: Merge Multiple Files, Adjustable Impact
- DEMO

BY VULN CODE

- XMLTableStats.java - Works with Nessus V2 Files
  - Available @ www.blackhat.org today.
- Command-Line: java XMLTableVuln *.nessus > output.xls
- Features: Merge Multiple Files, Vuln Priority Score
- DEMO

QUESTIONS?

Contact Info

Twitter: @jasonmoliver

Site: http://www.blackhat.org