Metricon ‘06

Leading Indicators in Information security

John Nye

August 1, 2006

Leading Indicators

- In Medicine
  - Body temperature
    - Elevated values indicate probable illness and severity
    - Temperature alone can not diagnose the illness
- Characteristics
  - Inexpensive to collect
  - Accurately diagnose the presence of the condition
  - May or may not reveal the nature of the condition

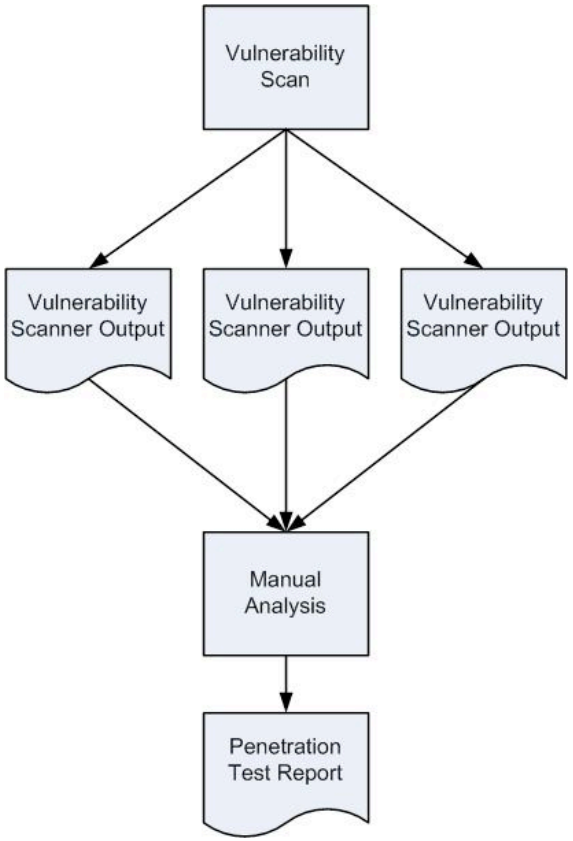
Leading Indicators in Information Security

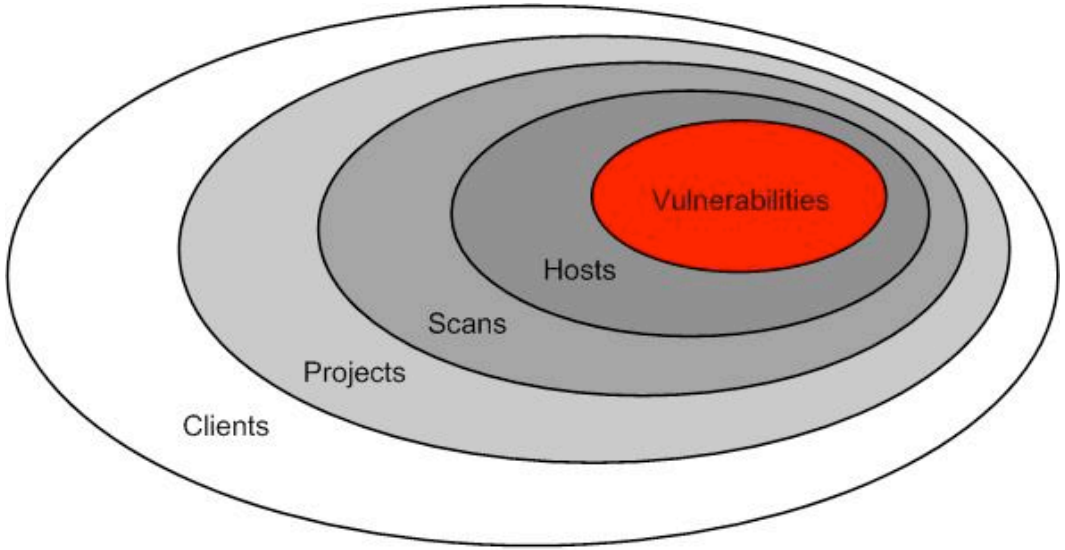
- Are there easily measured system attributes that predict an insecure configuration?
- For example, does having a large number of open ports correlate to having an insecure environment?

Application

- Evaluate an environment for its degree of vulnerability/risk to determine if additional investment is warranted (for example conducting a full vulnerability assessment)

Symantec Attack Center





Scans:
Date

Vulnerability:
Type
Scanner Severity
Manual Severity
Business Impact

SYMC Attack Center – The Data Set

- Scans conducted between April, 2005 and July, 2006
  - Adoption of the tool has been increasing
  - Most scan results are relatively recent
- 449 Scans Conducted
- Mostly External Penetration Tests
- Nessus
- Set Selection – We Eliminated:
  - Suspected test scans (i.e. we were testing the AC, not a client)
  - Scans that weren't used to produce a report

Methodology - Identifying Leading Indicators

- Performed initial analysis using scans as the set
- Vulnerability Score = sum of vulnerability severities divided by host count (calculated for each scan)
- Scans ranked into quartiles based on vulnerability scores
- Vulnerability Saturation = count of instances of a particular vulnerability divided by host count (calculated for each quartile)
- Plotted each vulnerability's saturation from quartile to quartile and examined the results

Eliminating Vulnerabilities as Potential Leading Indicators

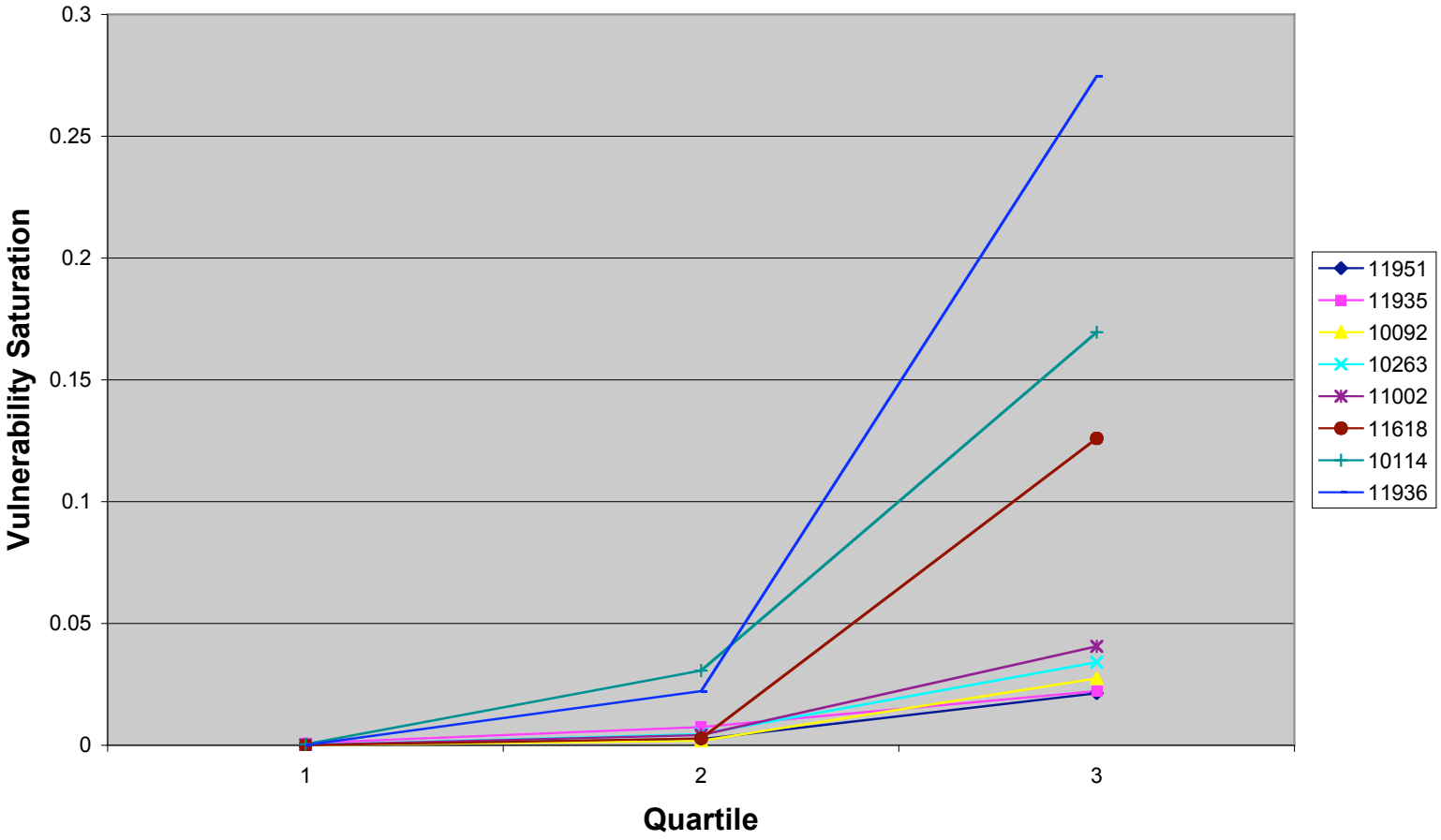
- Vulnerability eliminated from consideration if:
  - Highest quartile saturation did not exceed 2%
  - Saturation didn't increase with environment's vulnerability
  - Particular to a type of environment, not generic to most environments (i.e. Web vulnerabilities)

Real Problems with the Data Set – 11th hour

- Internal Network Scans
  - Had to eliminate most vulnerable quartile completely from the analysis because it contained multiple (and not-easily identified) scans conducted from within an enterprise perimeter
  - Probably eliminated several of the most vulnerable external scans in doing so

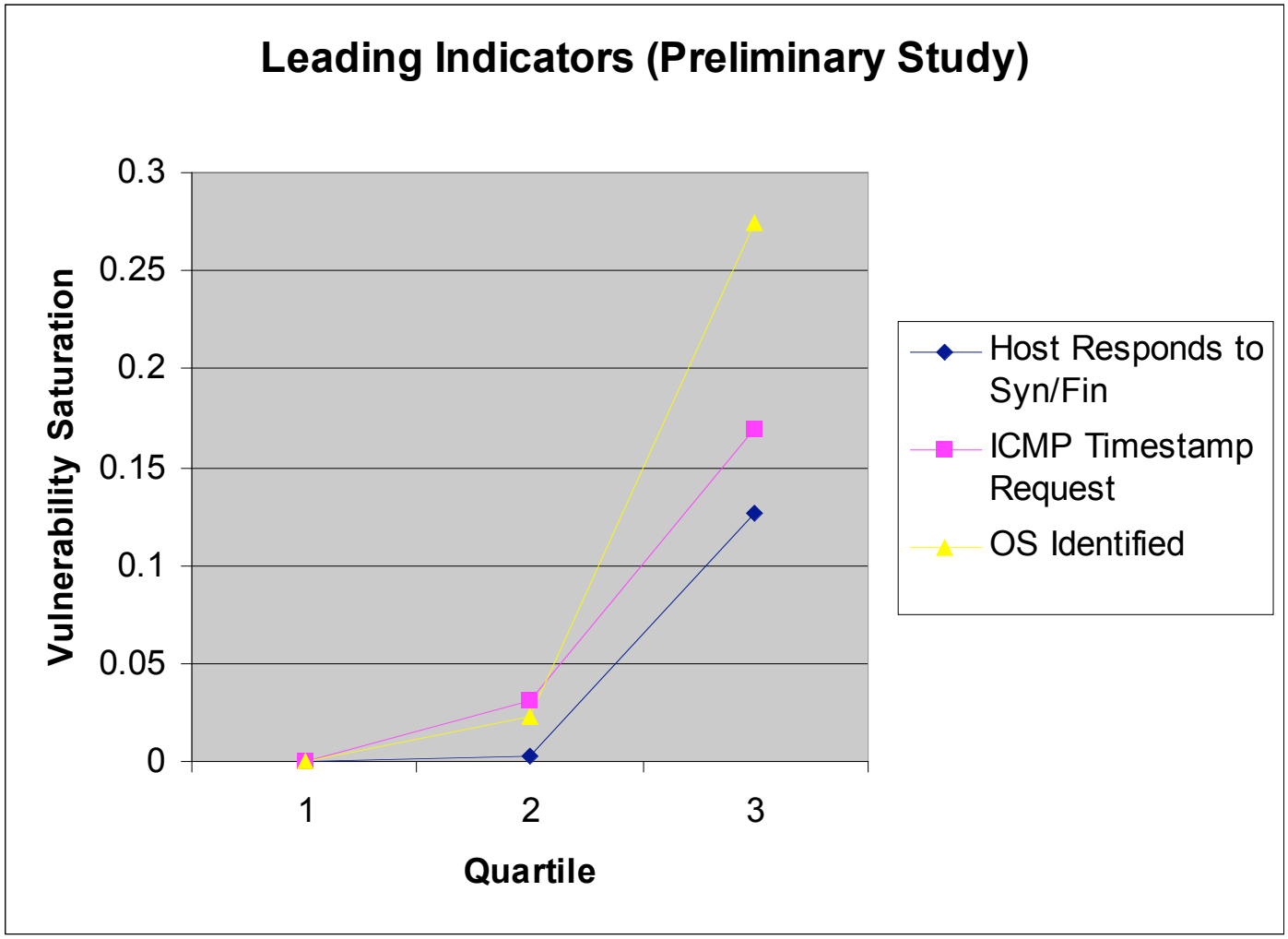
Findings (By Nessus Vuln ID)

Potential Leading Indicators

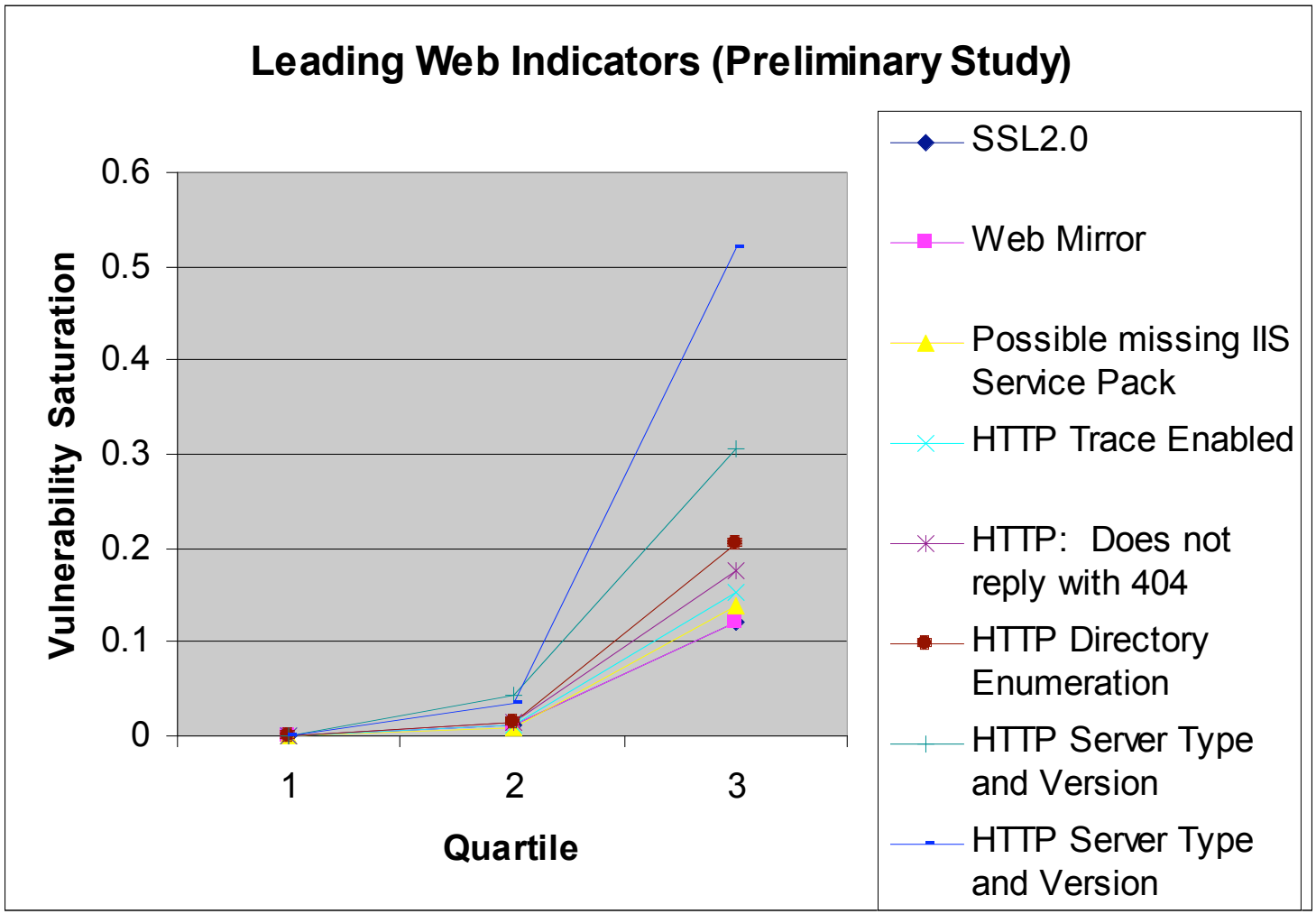


All non-Web scanner findings with a final saturation > 2% identified during remote penetration tests.

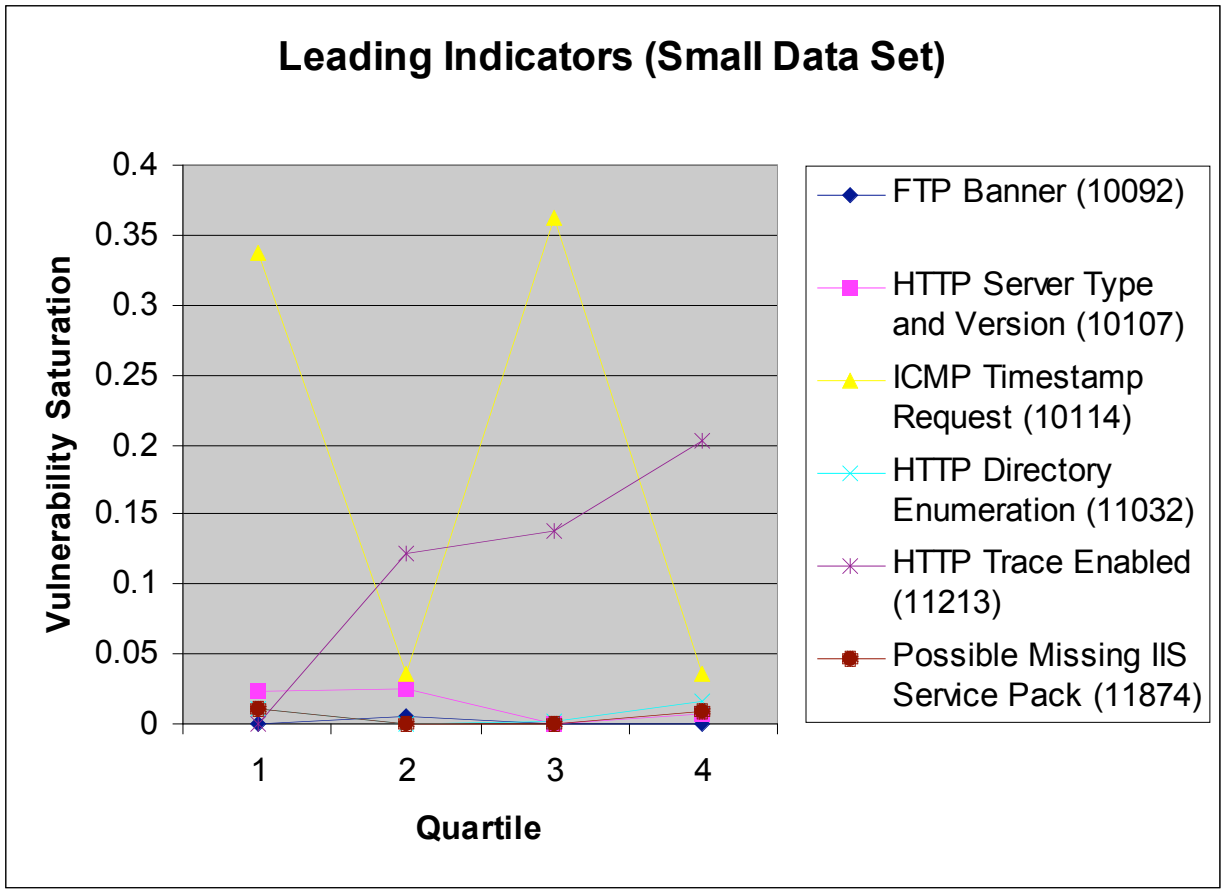
Top General Indicators



Top Web Indicators



Correlation: Scans vs. Project Reports



•All data is from external penetration tests
Small sample space
Top 8 general and top 8 Web vulnerabilities depicted (only 6 of the 16 were present in this data set.

Next Steps

- Clean up the data set
  - Quartile ranking of project reports doesn't match that of Scans
  - Mix of internal and external scan data
  - Small sample set of project reports
- Upgrade the math
  - Statistical regression
  - Multi-vulnerability analysis
- Repeat analysis for different types of environment
  - Internal vs. External, Web vs. Generic, etc.
- Implement the analysis directly in the Attack Center

Dangers with Leading Indicators

- The leading indicator itself can not be used as a diagnosis
- Gaming the system
  - Administrators may attempt to resolve only those vulnerabilities that are used as leading indicators.

Questions?

Thank You.

John Nye

Consulting Services Technical Lead

T. 617-768-2737

M. 617-501-3248

john_nye@symantec.com